Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais

Luiz Paulo Carvalho [2], Jonice Oliveira [2], Claudia Cappelli [2], Violeta Majer [1]

[1] Caixa Econômica Federal
[2] PPGI– Programa de Pós-graduação em Informática
Universidade Federal do Rio de Janeiro (UFRJ)
Avenida Athos da Silveira Ramos, 274 – Prédio do CCMN – Bloco C – Cidade Universitária, Rio de Janeiro – RJ, 21941-916

{luizpaulocarvalhodasilva ✉, claudia.cappelli}gmail.com

jonice@dcc.ufrj.br, violeta.majer@caixa.gov.br

Abstract. *Society is influenced by new technologies, culminating in new ethical issues. How to enable data protection in an era in which algorithms use it for whatever the purpose it may have? The Brazilian government, motivated by this issue, sanctioned a comprehensive legislation for data protection. In its writing the concern for transparency is clear. Noting this, what will be the technological issues associated with transparency in a privacy law?*

Resumo. *A sociedade é influenciada por novas tecnologias, culminando em questões éticas inéditas. Como habilitar a proteção de dados em uma época de algoritmos que utilizam os mesmos sabe-se lá para quê? O governo brasileiro, motivado por esta questão, sancionou uma legislação abrangente para proteção de dados. Na sua redação fica nítida a preocupação com a transparência. Em vista disso, quais serão as questões tecnológicas associadas com a transparência em uma lei dedicada à privacidade?*

1. Introdução

Com o avanço tecnológico e seu respectivo impacto social, surgem novas questões éticas [MOOR, 2005], motivando a criação ou atualização de legislações no contexto pertinente. Em 2015, uma firma de consultoria britânica chamada *Cambridge Analytica* acessou dados pessoais de 87 (oitenta e sete) milhões de usuários da rede social digital Facebook para analisar e influenciar o comportamento de eleitores nos Estados Unidos da América (EUA) [ISAAK E HANNA, 2018]. No Brasil, em 2014, a empresa de telecomunicação Velox foi acusada de, ilegalmente, vender dados pessoais de seus clientes a terceiros, culminando em multa de R$3,5 milhões [ZANATTA, 2015].

A Constituição Federal reconhece o direito fundamental à vida privada e intimidade e à liberdade de expressão [BRASIL, 1988], isto é, garantia da privacidade dos dados da pessoa natural e seu direito de instrumentalizá-los, como seus. No caso do Facebook ou da Velox, o cidadão não tem o controle, ou gerência, sobre seus próprios dados pessoais. Os dados podem ser utilizados para fins que seu titular não tenha noção, como entrada para algoritmos de tomada de decisão que incidem sobre o seu próprio futuro, venda de dados, análises comportamentais, e outros.

Observando a proporção da influência e valor dos dados pessoais na sociedade, consequentemente as suas implicações éticas [MOOR, 2005], foi criada a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção dos Dados Pessoais (LGPDP).

A LGPDP trata da proteção de dados como regra, sendo um dos objetivos principais da legislação, em seu Art. 1º [BRASIL, 2018a]. O conceito de privacidade [1], como particular, remete ao inverso de transparência, como abertura. Sua influência abrange todos os dados pessoais coletados, armazenados e processados por organizações públicas e privadas, com alcance internacional. A Lei de Acesso à Informação (LAI) [BRASIL, 2011], por sua vez, trata a transparência como regra.

O *Gartner Group* considera Ética Digital e Privacidade uma tendência tecnológica estratégica para 2019 [GARFINKEL, 2018]. Privacidade está presente em dois dos quatro grandes temas de desafios de pesquisa para Sistemas de Informação no Brasil de 2016 a 2026, Transparência possui um desafio próprio [BOSCARIOLI et al., 2017].

Este trabalho tem o objetivo de elencar futuros desafios para área de Transparência em Tecnologia de Informação e Comunicação (TIC) associados e oriundos da LGPDP, propondo uma agenda de pesquisa. O foco será o aspecto de TIC em SI [STAIR E REYNOLDS, 2018], composto de software, hardware, armazenamento de dados e redes.

O artigo é estruturado da seguinte forma, a Seção 2 discorre sobre Transparência; a Seção 3 aborda legislações pertinentes, associadas com transparência, e um exemplo real de sua influência; Seção 4 elenca a agenda de pesquisa; e Seção 5 apresenta discussão e conclusão.

2. Transparência

Holzner e Holzner (2006) definem Transparência como o fluxo aberto de informações, dependendo do acesso à informação presumidamente verdadeira que é detida pelas autoridades. A Figura 1 ilustra o conjunto de características e sub características que habilitam a Transparência, e seus relacionamentos [CAPPELLI, 2009].

Acessibilidade é a capacidade de ser acessado; usabilidade, capacidade de ser usado; informativo, capacidade de informar; entendimento, capacidade de ser entendido; e auditabilidade, possibilitar a capacidade de exame analítico [CAPPELLI, 2009]. Esta estruturação abarca três contextos [LEITE E CAPPELI, 2010]: **transparência organizacional**, interna, com foco nas partes interessadas nas organizações; **transparência alvo**, externa, com foco em partes interessadas específicas, fora do escopo organizacional; **transparência social**, externa, dedicada à ampla parcela da sociedade. E duas formas: **transparência passiva**, as autoridades respondem à requisição de dados; **transparência ativa**, as autoridades disponibilizam os dados em meios e canais específico, em tempo integral [2].

Iniciativas de abertura de dados pelas autoridades podem ser divididas em três categorias: Direito de saber, Transparência direcionada e Transparência colaborativa [FUNG et al., 2007]. Neste trabalho, as duas categorias pertinentes são Direito de saber, o objetivo geral de informar o público e proteger-se contra ações arbitrárias; e

[1] https://www.dicio.com.br/privacidade/ Disponível em 07/05/2019

[2] http://bit.ly/2Jcatrp. Disponível em 07/05/2019

Transparência colaborativa, com a orientação centrada no usuário e um papel de facilitador do governo, a fim de criar informações adaptáveis, em tempo real e personalizadas, que reduzam os riscos e as falhas dos serviços.

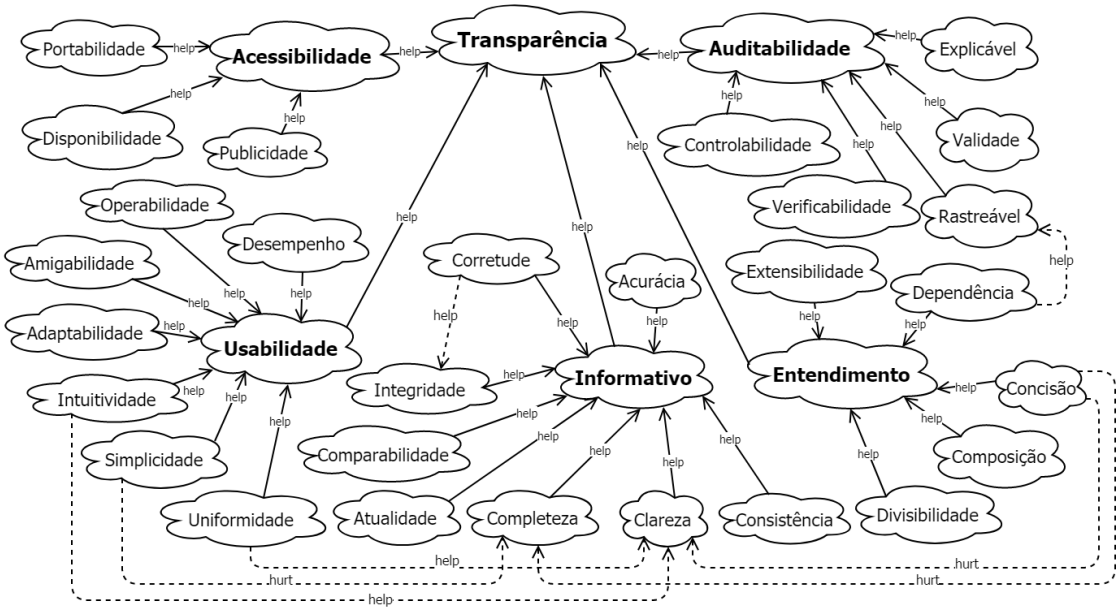

Figura 1: Transparência organizacional, proposto por Cappelli (2009)

3. Lei de Acesso à Informação e Lei Geral de Proteção de Dados Pessoais

A Lei nº 12.527, LAI [BRASIL, 2011], regula e determina o acesso às informações públicas brasileiras, a partir de transparência ativa e passiva, sendo a lei mais abrangente em significância vigente no Brasil sobre Transparência. Ela determina, em seu Art 3º, I: "observância da publicidade como preceito geral e do sigilo como exceção" [BRASIL, 2011]. No Art. 6º, VI, a lei determina assegurar proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

A Lei nº 12.965, Marco Civil da Internet (MCI) [BRASIL, 2014], estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil. No Art. 3º, II e III, figura a proteção à privacidade e dados pessoais. Entretanto, a LGPDP que dispõe e especifica o aspecto de privacidade e dados pessoais, nos meios físicos e digitais.

A LGDPD evoca problemas éticos associados com questões de humanidades digitais de impacto social, como Direito à Explicação [MONTEIRO, 2018], Direito à Autodeterminação Informativa [ROCHA, 2015], Direito ao Esquecimento [ROCHA, 2015], *surveillance* [NETO et al., 2017], Direito à Intimidade [RAMINELLI E RODEGHERI, 2016]. Além das questões éticas, pressão internacional exercida pela *General Data Protection Regulation* (GDPR) [3] da União Europeia (UE) foi uma motivação, definindo que apenas organizações de países com um nível maior ou igual de rigor para proteção de dados em legislação podem armazenar dados pessoais dos cidadãos

[3] https://eur-lex.europa.eu/eli/reg/2016/679/oj. Disponível em 07/05/2019

da UE, impactando, por exemplo, diretamente os negócios brasileiros [4]. A LGPDP vai além da GDPR, expandindo o escopo da proteção de dados [MONTEIRO, 2018].

A LAI abrange apenas organizações públicas, LGPDP inclui as privadas. A multa simples para infração pode chegar a R$50 milhões de reais [BRASIL, 2018a]. De acordo com o Art. 42º, II, § 2º, dependendo do contexto, o ônus da prova pode ser invertido, isto é, a culpa é transferida do titular dos dados para organização envolvida.

A LGPDP, no Art. 6º, VI, determina o princípio da transparência: "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;" [BRASIL, 2018a]. O termo "transparência" ou "transparente" tem cinco ocorrências no texto da legislação. O termo "clara", em relação à sub característica de "clareza", tem oito ocorrências. Outros termos, ou sinônimos, com os construtos da Figura 1 também ocorrem associados à "informação", em menor quantidade, como "completa", "objetiva", "atualizada", "inequívoca", "precisa", entre outros. O termo "acessível" ocorre no âmbito de transparência, da Figura 1, ou tradicionalmente sendo a utilização pela pessoa deficiente ou com mobilidade reduzida.

A LGPDP possui características específicas, que não a enquadram diretamente nas categorias de Direito de saber, Transparência direcionada ou Transparência colaborativa [FUNG et al., 2007]. Algoritmos opacos facilitam práticas abusivas, discriminatórias e monopolísticas, de complexa identificação, influenciando negativamente em direitos como pleno emprego, saúde, cidadania, dentre outros., criando uma assimetria entre indivíduos e organizações públicas ou privadas [MONTEIRO, 2018]. Outros problemas: comércio de dados pessoais, pois sistemas com termos de uso ou privacidade propositalmente complexos e extensos conduzem o cidadão à desinformação, permitindo a probabilidade de que o mesmo aceite, sem a devida noção, alguma cláusula de uso irrestrito dos seus dados; solicitação de dados oportunista, onde organizações coletam dados sem nenhum vínculo com o serviço em questão, para fins espúrios como comércio de dados, justificando que o titular inseriu os dados "por livre e espontânea vontade" [TANNER, 2013].

Na LGPDP, algoritmos opacos não precisam ser ativamente transparecidos; não precisam ser entregues integralmente por sigilo comercial ou industrial; não há colaboração ou envolvimento do cidadão com o algoritmo; e a lei estipula requisitos não-funcionais com foco no público-alvo, como clareza e concisão; caracterizando-a parcialmente como Transparência colaborativa. Como o cidadão só é exposto aos procedimentos, algorítmicos e automatizados ou não, que lhe convém, apenas devem ser abertas estas informações ao mesmo, passivamente, caracterizando Direito de saber. Logo, a legislação pode ser enquadrada nas duas categorias.

No Art. 2º, II da LGPDP é exposto o fundamento da autodeterminação informativa. Lorenzetti (2004) define como faculdade de dispor e optar por revelar dados de sua privacidade em todas as fases da elaboração e uso dos dados. Consciente, o titular pode permitir a agentes de tratamento o uso de seus dados pessoais livremente, desde que estes usos estejam transparentes ao mesmo.

[4] https://www.conjur.com.br/2018-fev-11/flei-protecao-dados-europa-pressiona-brasil-regular-tema. Disponível em 07/05/2019

Com objetivo de ilustração, é apresentado um exemplo de operacionalização de lei de proteção de dados em um sistema computacional na UE, a legislação brasileira ainda está em período de vacância legal. Dedicado exclusivamente à Autoridade Nacional de Proteção de Dados (ANPD), o Art. 55º entrou em vigor a partir 28 de dezembro de 2018, e o restante da legislação em 14 de agosto de 2020 [BRASIL, 2018b].

O exemplo selecionado é do website *information-age* [5], do Reino Unido. Um portal de informações sobre tecnologia, onde não há solicitação de cadastro ou qualquer dado pessoal dos seus usuários. Ao acessá-lo, a mensagem exposta na Figura 2 surge na parte inferior da tela. O usuário deve aceitá-la, podendo ver informações adicionais, em "*Show purposes*".

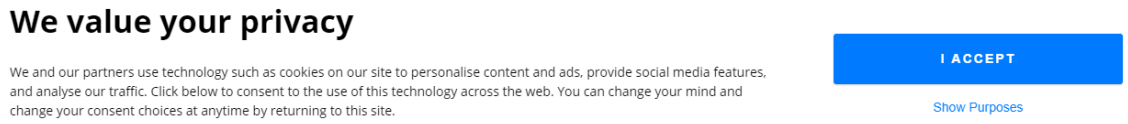

Figura 2: Interface de notificação ao acessar o website [5]

A Figura 3 expõe a captura de tela do consentimento de uso dos dados pelo usuário. Por padrão, todos não estão selecionados, isto é, se o usuário selecionasse "I accept" na interface anterior ele estaria rejeitando todos os usos, de todos fornecedores.

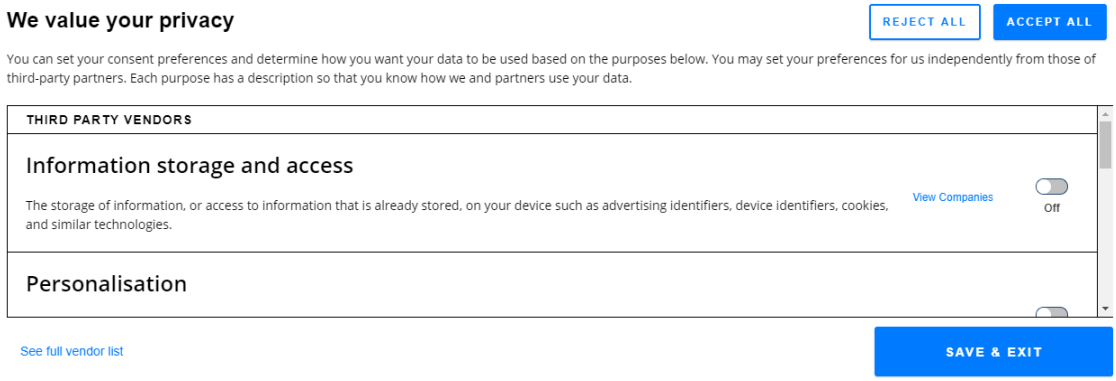

Figura 3: Interface de usos para os dados pessoais do usuário [5]

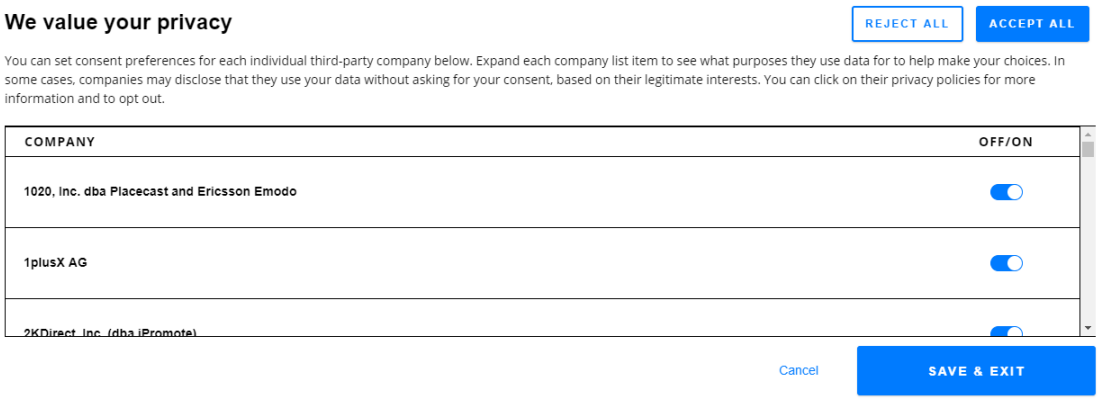

Figura 4: Interface de fornecedores passíveis de utilizar dados do usuário [5]

[5] https://www.information-age.com/ Disponível em 07/05/2019

A Figura 4 expõe a lista completa de fornecedores terceirizados, alertando também que os mesmos podem utilizar dados de maneira particular, sem consentimento do usuário. São, no total, 486 (quatrocentos e oitenta e seis) fornecedores terceirizados.

4. Encaminhamento à uma agenda de pesquisa

Esta seção encaminha possíveis desafios de pesquisa associando e analisando Transparência na LGPDP, no aspecto de TI de SI. A LGPDP é mais extensa e rigorosa do que a GPDR [MONTEIRO, 2018].

Itens da LGPDP associados com o contexto ou conceito, de maneira conotativa ou denotativa, de Transparência serão destacados e analisados pontualmente. Pelo alto nível de abstração da legislação, itens serão associados com características associadas à Transparência, Figura 1, abstraindo mecanismos e operacionalizações.

Art. 1º: *"Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado [...]*". Obrigatoriamente um SI não precisa envolver um sistema computacional [STAIR E REYNOLDS, 2018], isto é, mesmo que as pessoas referidas neste trecho armazenem ou transformem dados pessoais de terceiros em meios não digitais, a lei é integralmente válida. Por exemplo, empresas não poderão simplesmente captar dados pessoais de cidadãos na rua sem conformidade com a LGPDP, mesmo que com formulários físicos.

Art. 6º, IV: "*livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;*". **Acessibilidade**, Disponibilidade; **Informativo**, Integridade e Atualidade. Como habilitar a facilidade, a partir da forma e duração dos dados pessoais tratados com integralidade? Como respeitar e viabilizar a "gratuidade"?

Art. 6º, VI: "*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;*". **Acessibilidade**, Disponibilidade; **Informativo**, Clareza e Acurácia; **Usabilidade**, Adaptabilidade. Neste item o desafio se refere à comunicação de procedimentos, algorítmicos e automatizados ou não, sem conflitar com os segredos comercial e industrial. Algoritmos são ativos organizacionais [MOORE, 2017], organizações privadas não podem simplesmente transparece-los. Há necessidade da Adaptabilidade, seja para o público-alvo ao qual será comunicado, seja para proteger seu valor e propriedade.

Art. 8º, § 4, "*O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.*". **Informativo**, Acurácia; **Entendimento**, Divisibilidade. Como dividir, sem generalizar e de forma determinada, serviços associados com dados pessoais a serem tratados?

Art. 9º: "*O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva [...]*", seus incisos. **Acessibilidade**, Disponibilidade; **Usabilidade**, depende do caso específico; **Informativo**, Completeza. Ostensivamente, as informações devem ser completas. O conceito de "adequada" varia pelo uso, podendo ser associada com qualquer subcaracterística de Usabilidade. Especificamente no inciso V: "*informações acerca do uso compartilhado de dados pelo controlador e a finalidade;"*, assim como no exemplo da Seção 3, todos os parceiros (fornecedores) e finalidades devem ser expostos, este é um desafio especificamente para governança e transparência, pelas eventuais mudanças.

Art. 9º, VII, § 1: "*Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.*". Como habilitar a transparência de maneira não abusiva, enganosa, obscura ou equivocada? Como usuário, como detectar esses fenômenos e audita-los?

Art. 12º: "*Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.*". **Auditabilidade**, Rastreável. Como garantir que dado pessoal não sofrerá tratamento reverso ou inferência cruzada para que o anonimato seja garantido? Isto é, como transparecer dados considerando o Art 5º, I: "*dado pessoal: informação relacionada a pessoa natural identificada ou identificável;*"?

Art. 14º, § 6, "*As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.*". **Usabilidade**, Simplicidade e Adaptabilidade; **Informativo**, Clareza. Este é o caso onde "acessível" não se refere à Acessibilidade de Transparência. Como transparecer, de maneira simples e clara, informações de tratamento de dados para crianças e adolescentes específicas? Garantindo sua autonomia, nos casos pertinentes.

Art. 18º: "*O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:*", seus incisos e parágrafos. Envolve todos os elementos de Transparência, na Figura 1. Como as organizações realizarão a gestão de transparência de dados relacionados a todos os direitos presentes neste artigo ao titular de dados? Como controlar não apenas os dados pertinentes ao escopo organizacional, como (i) informações que possam vir a ser solicitadas pelos titulares de dados sobre a manutenção de seus próprios dados? (ii) rastreamento de todos os fornecedores com os quais dados pessoais dos titulares são compartilhados?

Art. 19º: "*A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:*", seus incisos e parágrafos. Similar ao Art. 18º. **Usabilidade**, Simplicidade, Adaptabilidade e Operabilidade. **Informativo**, Clareza e Completeza. Como gerenciar os dados pessoais dos titulares de maneira que eles estejam prontamente disponíveis, inclusive para formato impresso, e interoperáveis para outros tratamentos de dados?

Art. 20º: "*O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.*". **Auditabilidade**, todas as características. Como garantir ao titular o Direito à Explicação transparente, sem afetar segredos comerciais e industriais, sobre procedimentos relacionados com seus dados pessoais e que impactem seus interesses particulares?

A Seção I é dedicada exclusivamente ao tratamento de dados pessoais pelo poder público. São seis referências à LAI e outras legislações adjacentes, expondo a importância dada ao tema de Transparência e interoperação entre as leis.

O Art. 24º e seu parágrafo único devem ser analisados com cautela, vista a divisão entre categorias de organizações e suas relações com dados pessoais, isto é, empresas públicas e sociedades de economia mista atuando em regime de concorrência.

Art. 25º: "*Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado* [...]". **Acessibilidade**, Portabilidade; **Usabilidade**, Operabilidade e Adaptabilidade; **Entendimento**, Extensibilidade. Como habilitar a transparência interoperável e manter o Direito à Intimidade e privacidade?

Art. 41º: "*O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.*". **Informativo**, Clareza e Concisão. Como transparecer ao titular de dados com quem ele deverá comunicar-se em relação aos seus próprios dados?

O Art. 44º, e seus itens, determina uma lógica deôntica sobre a atividade dos agentes de tratamento, suas responsabilidades e "boa fé". Deve ser transparecido o modo, técnicas, resultados e riscos do tratamento com a respectiva época realizada. Não há métrica de Transparência diretamente associada com estas informações. A redação do artigo é vaga e sua semântica é dúbia, todos os tratamentos devem conter essas informações sobre os mesmos? Como transparecer as técnicas? Técnicas para qualquer tratamento? O que seria "modo pela qual é realizado"?

Art. 48º: "*O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*", seus incisos e parágrafos. **Acessibilidade**, Publicidade. **Auditabilidade**, todos. **Usabilidade**, Amigabilidade. **Informativo**, Atualidade. Como transparecer que dados foram alvo de incidente de segurança, de forma amigável, explicativa, datada e publicizada apenas sobre dados pessoais específicos dos titulares afetados?

Nesta Seção a LGPDP foi submetida às características de Transparência e expostos desafios, como questões, ao aspecto tecnológico de SI. Pontos da legislação tangenciam aspectos tecnológicos envolvidos com humanos e procedurais de SI. Por exemplo, na UE surgiu o profissional especializado na GDPR, o Administrador de Proteção de Dados (*Data Protection Officer* - DPO) [6], que necessita de conhecimento tanto de TI, como em legislação, auditoria e no negócio envolvido. Na LGPDP são determinados cargos de controlador, operador e encarregado; sendo este último o equivalente brasileiro ao DPO europeu.

5. Discussão e conclusão

Este trabalho busca abrir uma agenda de pesquisa abordando a LGPDP, Transparência e possíveis desafios para o aspecto de TI em SI. Os desafios servem tanto para transparência organizacional, interna, como social, externa; por exemplo, como habilitar entendimento em termos de privacidade? Em algoritmos? Como governar dados para que os mesmos estejam prontamente transparentes à requisição dos titulares?

Mark Zuckerberg, chefe executivo do Facebook, publicou no próprio Facebook uma nota pessoal, "*A Privacy-Focused Vision for Social Networking*" [7], expondo um discurso "favorável" à privacidade e proteção de dados. Controverso, o mesmo aponta a

[6] https://en.wikipedia.org/wiki/Data_Protection_Officer. Disponível em 07/05/2019
[7] http://bit.ly/2CALrND. Disponível em 07/05/2019

responsabilidade do Facebook em prevenir “atos terríveis”, como exploração infantil, terrorismo e extorsão, e de agir com agentes da lei para tal. Como o Facebook vai prever comportamentos e ações humanas sem permissão de instrumentalizar dados pessoais dos seus usuários para este fim? E a criptografia ponta-a-ponta? O que significa “através de padrões de atividades e outros meios”, sem dados pessoais? Estas são questões com direcionamento aplicado, a partir de interpretações obscuras para “atos terríveis”.

Cabe ressaltar que o Art. 4º, II, b, determina que a LGPDP não se aplica ao tratamento de dados pessoais realizados para fins exclusivamente acadêmicos. Entretanto, com maior restrição e controle ao tratamento, incluindo coleta e armazenamento, de dados pessoais pode vir um impacto negativo em pesquisas baseadas em monitoramento, mineração e coleta, automatizado ou não, de dados.

Não há consenso na definição de Transparência na literatura [CAPPELLI, 2009], a requisição da qualidade de transparência, sem defini-la (Art. 5º), configura um problema conceitual. Este trabalho associa o requisito de transparência, presente na lei de forma recorrente, com as respectivas características de Transparência.

A LGPDP possui interesses semânticos e parcialmente conflitantes, uma busca automatizada por legislações, como em Engiel et al. (2016), associadas com “Privacidade” ou “Transparência” podem retorná-la, sendo que a mesma restringe o acesso aos dados em alguns pontos e determina a abertura em outros, simultaneamente.

Neste trabalho foi realizada uma análise apenas pelo aspecto de TI em SI, um trabalho futuro pode propor nortes de pesquisa ao aspecto humano e procedural. Outros trabalhos futuros são o aprofundamento em cada questão exposta neste trabalho, relacionando-a com um componente de TI específico e abordagens já utilizadas por outros países; comparação entre GDPR e LGPDP pelo viés tecnológico; desenvolvimento de artefatos que apoiem organizações, internamente, e cidadãos, externamente, a lidar com a LGPDP; acompanhamento do trabalho da Agência Nacional de Proteção de Dados em suas competências (Art. 55-J) [BRASIL, 2018a].

6. Referências

Todas as referências online neste trabalho estavam disponíveis em 07/05/2019.

Boscarioli, C., Araujo, R. M., Maciel, R. S. P. (2017) "I GranDSI-BR – Grand Research Challenges in Information Systems in Brazil 2016-2026" Special Committee on Information Systems (CE-SI). Brazilian Computer Society (SBC).

Brasil (1988) CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Disponível em: http://bit.ly/2QTSWVj

Brasil (2011) LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Disponível em: http://bit.ly/2HPS1Di

Brasil (2014) LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Disponível em: http://bit.ly/2CBJrVk

Brasil (2018a) LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: http://bit.ly/2YgUqMZ

Brasil (2018b) MEDIDA PROVISÓRIA Nº 869, DE 27 DE DEZEMBRO DE 2018. Disponível em: http://bit.ly/2TvhsMy

Cappelli, C. (2009) "Uma Abordagem Para Transparência Em Processos Organizacionais Utilizando Aspectos". Tese de Doutorado em Informática, PUC-Rio, Brasil.

Engiel, P., Portugal, R., Leite, J. C. S. P. (2016) "Descobrindo Projetos de Lei relacionados a Transparência". V Workshop de Transparência em Sistemas. Rio de Janeiro, Brasil.

Fung, A., Graham, M., Weil, D. (2007) "Full Disclosure: The Perils and Promise of Transparency". Cambridge University Press, EUA.

Garfinkel, J. (2018) "Gartner Identifies the Top 10 Strategic Technology Trends for 2019". Disponível em: https://gtnr.it/2Fs2Ubu

Holzner, B., Holzner, L. (2006) "Transparency in Global Change: The Vanguard of the Open Society". 1ª edição. Universidade de Pittsburgh, EUA.

Isaak, J., Hanna, M. J. (2018) "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection". IEEE, Computer 51 (8), pp. 56-59.

Leite, J. C., Cappelli, C. (2010) "Software Transparency". Business & Information Systems Engineering 2 (3), pp. 127-139.

Lorenzetti, R. (2004) "Comércio Eletrônico". Revista dos Tribunais. São Paulo, Brasil.

Monteiro, R. (2018) "Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?". INSTITUTO IGARAPÉ, Artigo Estratégico 39. Rio de Janeiro, Brasil.

Moor, J. H. (2005) "Why we need better ethics for emerging technologies". Ethics and Information Technology 7, pp. 111–119. doi: 10.1007/s10676-006-0008-0.

Neto, E., Morais, J. L., Bezerra, T. (2017) "O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos". Direito e Mundo digital 7 (3), pp. 185-199.

Raminelli, F., Rodegheri, L. (2016) "Proteção de Dados Pessoais na Internet no Brasil: Análise de Decisões Proferidas pelo Supremo Tribunal Federal". Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS XI (2), pp. 89-119.

Rocha, E. (2015) "O Direito à Autodeterminação Informativa e a Proteção de Dados Pessoais". Monografia de Bacharelado em Direito, UFRGS, Brasil.

Stair, R. M., Reynolds, G. W. (2018) "Principles of Information Systems" 13ª edição. Cengage Learning, EUA.

Tanner, A. (2013) "Never Give Stores Your ZIP Code. Here's Why". Revista FORBES. Disponível em: http://bit.ly/2UWih2w

Zanatta, R. (2015) "A Proteção de Dados entre Leis, Códigos e Programação: os limites do Marco Civil da Internet". Em: De Lucca, N., Simão Filho, A., Lima, C. Direito e Internet III: Marco Civil da Internet. São Paulo: Quartier Latin, p. 447-470.