Os desafios éticos do profissional da informação face à vulnerabilidade dos dados pessoais: uma reflexão a partir da perspectiva brasileira

Los desafíos éticos del profesional de la información y la vulnerabilidad de los datos personales: una reflexión a partir de la perspectiva brasileña

The vulnerability of personal data and the ethical challenges of the information professional: a Brazilian perspective

José Augusto BAGATINI, José Augusto Chaves GUIMARÃES

Universidade Estadual Paulista - UNESP, Depto de Ciência da Informação, Av. Higino Muzzi Filho, 737, Marília, SP, 17525-900,Brasil; jose.bagatini@unesp.br, guima@marilia.unesp.br

Resumen

Se discute el papel y el desafio ético del profesional de la información (principalmente, del archivero y el bibliotecario) en garantizar la protección de datos personales y prevenir daños al ciudadano y a la sociedad como resultado de su uso ilegítimo. El ciudadano, al usar cotidianeamente soluciones informatizadas, deja rastros de su comportamiento, que se deben interpretar como datos personales, ya que se refieren a sus actos y revelan características físicas o de personalidad. Estos datos pueden considerarse actualmente como un bien intercambiado en el mercado de la vigilancia. Sin embargo, aún no existe en Brasil una discusión que permita situar, de forma sistematizada, los datos personales como un bien vulnerable a acciones invasivas o fraudulentas.

Palabras clave: Datos personales. Ética de la información. Vigilancia digital. Fuga de datos. Brasil.

Abstract

The challenges and ethical role of the information professional (notably the archivist, record manager and librarian) is discussed to ensure the protection of personal data and to prevent harm to the citizen and the society. The citizen, with the daily use of computerized solutions, began to create a greater amount of traces of their behaviors, which can be interpreted as personal data as they refer directly to their actions and reveal its physical or personality characteristics. Nowadays, these data can be considered as a special kind of commodity at the surveillance market. However, there is still no discussion in Brazil that allows us to situate personal data in a more systematic way as something that is vulnerable to invasive or fraudulent actions.

Keywords: Personal data. Information ethics. Digital surveillance. Data breachs. Brasil.

1. Introdução

A Ciência da Informação, que tem no dado a matéria prima de seu objeto, a informação, desde o seu nascedouro revelou uma forte vinculação com a dimensão tecnológica, como se pode observar tanto na concepção Otletiana de Documentação, hoje considerada como precursora da Internet (Otlet, 1934) como também, e principalmente, com o advento dos computadores, na preocupação de Vannevar Bush (1945) em dotar o homem de "memórias auxiliares" que contribuíssem para o armazenamento e o processamento de enormes volumes de dados.

Nesse contexto, há de se destacar, mais especialmente, a partir da década de 1990, a popularização da internet, tecnologia responsável por uma profunda transformação na forma com que o homem contemporâneo se relaciona com quase tudo. O cidadão, ao fazer uso constante de soluções informatizadas, seja para realizar compras, ler notícias ou requisitar atendimento nos órgãos governamentais, passou a produzir dados comportamentais sobre si mesmo numa escala jamais vista, rastros esses, que podem ser interpretados como dados pessoais, pois possuem vínculo direto com o usuário desses sistemas uma vez que se referem a seus atos e revelam características físicas ou de personalidade (Doneda, 2011).

Rapidamente o mercado eletrônico encontrou nos dados pessoais um meio pelo qual as atividades de marketing poderiam se tornar mais efetivas, haja vista que, tais dados ao serem tratados podem indicar novas necessidades humanas ou a propensão de um segmento populacional consumir um determinado produto já lançado, diminuindo assim os custos de campanhas publicitárias e de pesquisa e desenvolvimento de novos produtos. Nesse cenário surge empresas como Amazon e Google, que segundo Bauman e Lyon (2014) construíram seus modelos de negócio

voltados à vigilância. No caso da Amazon, tem-se a coleta e armazenamento de dados referentes a compras, listas de desejos, histórico de busca, histórico de navegação e etc. de seus clientes para montar o perfil do mesmo conseguindo, assim, de forma menos custosa indicar produtos e serviços que tenham maior probabilidade de sanar uma necessidade ou desenvolver uma nova. A Google, por sua vez, oferece serviços gratuitos como agenda, buscador, e-mail, espaço para armazenamento de arquivos digitais e redes sociais com o intuito de coletar o máximo de dados pessoais do usuário para, assim, compreender aspectos como padrão de consumo, estilo de vida, faixa etária, poder aquisitivo, vizinhança, rede de contatos, entre outros. Dessa maneira, monetiza os dados adquiridos fornecendo a possibilidade de anunciantes exibirem publicidade direcionada aos usuários de serviços Google, possibilitando assim, outras companhias elevarem sua taxa de conversão (concretização de venda).

Com os altos rendimentos apresentados pelas empresas citadas e outras que se desenvolveram baseando-se no modelo de negócio voltado à vigilância, inevitavelmente os dados pessoais se tornaram um importante bem econômico e transformaram-se em moeda para pagar pelo uso gratuito de plataformas, sites e serviços (Silveira, Avelino e Souza, 2016).

Nesse conturbado contexto, questiona-se qual o papel do profissional da informação (bibliotecário, arquivista, etc.), para que possa não apenas garantir à sociedade o acesso à informação por ela produzida como também, e em outra direção, comprometer-se com a proteção dos cidadãos no que tange os dados de natureza pessoal cuja disponibilização e divulgação pode gerar danos de diferentes ordens.

A vista disso, parte-se de uma caracterização do mercado de informação na atualidade, e de como esse mercado vem muitas vezes ferindo questões ligadas à privacidade o que leva à abordagem da vulnerabilidade dos dados pessoais em um contexto de mercado de vigilância. Tais aspectos servem de subsídio a uma reflexão sobre o papel do profissional da informação – e os desafios por ele enfrentados – na atualidade no que se refere à proteção dos dados pessoais.

2. A vulnerabilidade dos dados pessoais e o *mercado da vigilância*

Os dados pessoais, na atualidade, passaram a ser um importante objeto de ação econômica, movendo vultosos mercados. Essa questão atinge, de maneira mais direta, a a privacidade do indivíduo, o que pode ocorrer nem sempre de forma direta e explícita mas, e principalmente, por meio de ações econômicas de duplo objetivo, como é o caso das trade-offs que, segundo Acquisti (2013) visam à resolução de problemas mas, em contrapartida, acarretam outros, obrigando a escolhas como abrir mão de algum bem ou serviço para se obter outro, no contexto do denominado mercado da privacidade. O referido autor descreve três modalidades de trade offs: 1) na compra de um bem comum, em que o consumidor pode fornecer dados durante a transação financeira; 2) no mercado de dados pessoais, em que os dados do indivíduo podem fazer parte da troca entre agentes e; 3) no mercado da proteção das informações pessoais, em que consumidores buscam produtos e serviços para gerenciar e proteger seus dados pessoais.

Nas hipóteses anteriormente citadas - os trade-offs previstos por Acquisti (2013) e a definição de dados pessoais como forma de pagamento pelo uso de plataformas gratuitas de tal como preconizado por Silveira, Avelino e Souza (2016) caracterizam a maneira pela qual se estabelece a relação de poder entre as empresas que fazem parte do denominado mercado da privacidade e a população, que depende dessas ferramentas para desempenhar suas atividades cotidianas. Observa-se, assim, que uma vigilância endêmica se instaurou como importante ferramenta no mercado da privacidade, gerando quantidades massivas de informações, de tal modo que o subproduto dessa captura em larga escala passa a residir nos grandes estoques informacionais.

Na seara dos dados pessoais tem-se em nossos dias, um novo mercado, denominado mercado da vigilância – e, por consequência, da privacidade – que de alguma maneira poderia ser inserido naquilo que Barreto (2000) denomina como mercado da informação. Para o autor, esse mercado possui característica peculiar quanto à relação entre oferta e demanda, na medida em que, nesse ambiente, “é a oferta que determina a demanda por informação” (Barreto, 2000 p. 27, grifo do autor). Logo, o constante armazenamento de dados pessoais por parte do mercado da privacidade aumenta consideravelmente a demanda por esse bem e, como resultado tem-se, entre outros, um loop, na medida em que companhias rastreiam e armazenam dados sobre a população e os fornecem para outras companhias que tenham interesse, em um movimento helicoidal.

O mercado da privacidade poderia ser comparado a um iceberg cuja ponta exposta pode ser representada por Amazon, Google e Facebook, que sabidamente coletam dados pessoais e os utilizam, mas esse nicho tem sua real dinâmica movida pela parte submersa do iceberg, representada pelas empresas data brokers (espécies

de “corretoras de dados”), especialistas em captura, processamento e venda de dados pessoais (Novaes, 2014).

A atividades dessas empresas, ainda não reguladas nos Estados Unidos, têm despertado preocupações. Em 2014, o órgão norte americano Federal Trade Comission - FTC produziu o relatório Data Brokers: A Call for Transparency and Accountability em que são discutidos os resultados levantados por um minucioso estudo sobre os nove maiores data brokers que atuam nos Estados Unidos (Creativante, 2014). O relatório foi utilizado como subsidio para embasar o pedido feito ao Congresso de que haja regulamentação das atividades econômicas dessas entidades.

A Acxiom, uma das companhias citadas no referido relatório acumula em média 1.500 informações sobre cada pessoa presente em sua base de dados, abrangendo 96% da população norte-americana (Pariser, 2012). A maior parte desse banco de dados é formada por informações coletadas sem o consentimento dos data subjects (cidadãos titulares dos dados coletados) que, em grande maioria, desconhecem a existência e atividades de empresas data brokers e não imaginam que seus dados são bens de consumo para um mercado de alta capitalização (Creativante, 2014).

No Brasil, a maior “corretora de dados” é a Serasa Experian que, segundo o seu próprio site, reúne os dados de mais de 2,3 bilhões de consumidores em mais de 29 países. Sua ferramenta, denominada Mosaic Brasil, “classifica a população brasileira em 11 grupos e 40 segmentos baseados em aspectos financeiros, geográficos, demográficos, de consumo, comportamento e estilo de vida” (Serasa Experian, 2014).

Segundo a própria Serasa Experian (2014), a proposta da ferramenta é ajudar empresas a compreender certos aspectos do consumidor — como perfil, necessidades, desejos e comportamentos — e assim fornecer insights para o desenvolvimento de estratégias de marketing e realização de ofertas segmentadas, prospecção, rentabilização da carteira de clientes, comunicação dirigida, modelagem estatística, estudos de mercado e geomarketing para ampliar oportunidades e auxiliar na tomada de decisões.

Dessa forma, o sujeito, quando registrado em um dos 11 grupos e 40 segmentos do Mosaic Brasil, passa a fazer parte daquilo que Pariser (2012) apresenta como bubbles, conjunto de pessoas agrupadas em banco de dados levando em conta a similaridade do estilo e padrão de vida. Essas bolhas são formadas por empresas do mercado da privacidade que, ao se valerem da vigilância, utilizam dados como renda, preferências de lazer, histórico de compra e rastros criados pela navegação e buscas na internet para dessa forma, executar o que atualmente é chamado por profilling – através da análise de comportamento alocar cidadão na bolha mais condizente com seu perfil (Silveira, Avelino e Souza, 2016).

Para Bauman e Lyon (2014), a vigilância é uma característica básica do mundo contemporâneo, que foge às nossas preocupações por encararmos a realidade como uma serie de relações distintas; entretanto, o mercado compreende que compartilhar dados é lucrativo e isso faz com que nosso comportamento seja encarado como mercadoria (Parise, 2012).

Sem leis específicas que regulem o mercado da privacidade, a relação de poder entre data subject e data holder (interessados em obter dados) continuará sendo desleal e benéfica à segunda parte. Para identificar a situação global perante à privacidade e à proteção de dados, o especialista em direito e políticas públicas David Banisar, mapeia projetos e leis já estabelecidas específicas sobre o tema e os publica anualmente no mapa “National Comprehemsive Data Protection/Privacy Laws and Bills” (Banisar, 2016).

O Brasil atualmente dispõe de uma estrutura dispersa e não específica sobre o tema proteção de dados, sendo que a proteção maior se dá no âmbito da privacidade e transparência, e não na proteção de dados em si (Lima e Monteiro, 2013). Exemplo disso reside na Lei de Acesso à Informação que trata, ainda que de forma tangencial, a questão da transparência da informação pública (Santos, 2016). Por esse motivo, desde 2010 discute-se o Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP) que, em seu Art. 1º, “dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.” (Brasil, 2016, p. 1). Trazendo a discussão mais especificamente para o universo da Ciência da Informação, observam-se discussões de diversas ordens, tais como: a) a questão da informação como um insumo e como algo que possui um valor (Araújo, 2010; Pinheiro, 2005; Pomart e Sutter, 2014; Sant’anna e Moreira 2016); b) os dados como subsídio à informação e ao conhecimento (Capurro, 2007; Xavier e Costa, 2010; Semidão, 2014); c) a informação pessoal como objeto de estudos, em especial no campo da Arquivologia, com a questão dos arquivos pessoais (Borges Fortes; Oro Boff, 2014; Lima, 2013; E Silva; Araújo; Azevedo, 2013); e a lei de acesso à informação e o habeas data (Bacellar Filho e Schier, 2013; Gil-Leiva e Moya Martínez, 2011; Rocha e Konrad, 2013).

No entanto, ainda não se tem, no Brasil, uma discussão que permita situar, de forma mais sistematizada, os dados pessoais como algo que, por conta do valor econômico que a eles possa ser atribuído, esteja vulnerável a ações invasivas ou fraudulentas.

O fato de os dados pessoais encontrarem-se cada vez mais vulneráveis, em virtude do modo pelo qual são amplamente coletados, armazenados e tratados, possibilita a ocorrência dos "vazamentos de dados com consequentes danos ao cidadão, ao extrapolar os limites do direito à privacidade.

Cumpre destacar que a questão do vazamento de dados constitui problema de maior importância na atualidade, haja vista que, de 2012 para 2013, houve um aumento de 62% no indicador de exposição indevida de dados pessoais, o que se traduz em 552 milhões de identidades expostas (Carraretto, 2014). Ainda segundo o autor, no ano de 2012 foi registrado um "mega" vazamento de dados, enquanto em 2013 foram oito, sendo as pequenas e médias empresas (PMEs) alvos-chave desses ataques. Esse setor foi contemplado pelo relatório ESET Security Report Latinoamérica 2016 em que cerca de 10% das PMEs questionadas afirmaram que sofreram acesso indevido à suas bases de dados (ESET, 2016). Segundo Carraretto (2014), os bancos de dados governamentais representam 16% de todas atividades relacionadas à roubo e vazamento de dados.

A vista disso, questiona-se qual o papel do profissional da informação no que tange ao desenvolvimento de ações que visem à proteção desses dados, de modo a impedir vazamentos e consequentes danos, sejam eles individuais ou sociais.

3. O profissional da informação em seu compromisso ético com a proteção dos dados pessoais

O profissional da informação tem por missão precípua reunir e organizar a informação para que ela esteja disponível e seja encontrada e apropriada pela sociedade (Smit, 1986), entendendo-se essa informação como algo simbólico e socialmente decodificável que possa gerar conhecimento individual e social e, para tanto, necessita estar materializado e socializado para garantir portabilidade no espaço e permanência no tempo (Smit, 1986; Smit e Barreto, 2002).

Desse modo, sua ação vai muito além de um conjunto de processos, produtos e instrumentos para, de forma mais ampla, revestir-se de uma dimensão ética cujo valor maior, como bem destacam Guimarães, Fernández-Molina, Pinho e Milani (2008) reside na promoção do acesso à informação. Tem-se, em suma, uma reflexão mais sobre o *bem agir* ou *bem fazer* desse profissional, a partir da especificidade dos saberes que lhe são inerentes, revelando as concepções e comportamentos que dele se espera e de onde decorrre sua responsabilidade profissional (Wecker e Adeney, 2000; SÁ, 2000, p. 15).

Com o crescente aporte tecnológico nas atividades informativas, essa dimensão ética da atividade profissional assumiu dimensões mais amplas, e em duas dimensões distintas: por um lado, no que tange ao combate à censura, como decorrência do direito à liberdade individual e, por outro, na proteção do direito à privacidade, uma vez que os meios tecnológicos, como já exposto, podem servir também a esse fim.

Guimarães (2000) identifica cinco compromissos éticos essenciais do profissional da informação: com o usuário, com a organização, com a informação, com a profissão e consigo mesmo enquanto cidadão e profissional.

Trazendo a questão para o universo da proteção dos dados pessoais, destaca-se o seguinte:

- o compromisso ético com o usuário, por referir-se não apenas à disseminação da informação mas, e principalmente, pela maneira como esse usuário se apropria da informação, reside nos cuidados com forma de disponibilização da informação no sentido de evitar apropriações deletérias;
- o compromisso com a organização se coloca, nesse caso, na prevenção de situações que possam levar a unidade de informação a ser imputada como cúmplice de uma ação ilegal ou mesmo antiética;
- o compromisso com a informação reside no respeito à própria natureza dessa informação, em especial atentando para situações em que essa informação assume caráter pessoal e cuja divulgação irrefletida pode gerar danos pessoais;
- o compromisso com a profissão está justamente na garantia de um fazer ético que contribua para o avanço social, científico e tecnológico, respeitando os direitos individuais, tal como o direito à privacidade; e
- o compromisso consigo mesmo enquanto cidadão e profissional reside na promoção de uma sociedade mais justa e inclusiva, pautada pelo respeito ao semelhante.

Vale aqui recordar os fatores elencados há mais de duas décadas por Froehlich (1994) como intervenientes nas decisões éticas do profissional da informação, nomeadamente: utilidade social,

responsabilidade social, sobrevivência organizacional, sobrevivência profissional, respeito por si mesmo, respeito pelos demais indivíduos e instituições, padrões coletivo-culturais e padrões legais.

A utilidade social refere-se ao compromisso com a comunidade usuária de modo a tornar-lhe disponível informação *passível de ser utilizada da melhor maneira possível* em seu dia-a-dia.

A responsabilidade social refere-se, por exemplo, ao compromisso com a disponibilização, aos usuários, de uma coleção o mais completa e equilibrada possível, distanciando-se de aspectos relativos a censura ou discriminação, por vezes determinados pelo ambiente externo. Aqui se alia, igualmente, o distanciamento de aspectos relativos à disseminação indiscriminada da informação quando esta trouxer prejuízos pessoais.

A sobrevivência organizacional guarda estreita relação com as políticas da própria instituição e, por vezes, colide com a utilidade social, enquanto a sobrevivência profissional trata das questões da própria profissão como salários e o próprio código de ética profissional, aqui incluindo-se a manutenção da boa imagem da profissão – o seu profissionalismo – o que decorre não apenas da manutenção de alto padrão técnico de atuação mas, também, da manutenção de alto padrão ético nas ações empreendidas.

O respeito por si mesmo, por sua vez, se constrói a partir da responsabilidade e da consciência das ações empreendidas.

Por sua vez, o respeito por outros indivíduos e instituições se situa, eticamente, na busca pela alteridade (colocar-se no lugar do outro) para melhor aquilatar possíveis efeitos deletérios de ações irrefletidas.

Froehlich (1994, p. 462) refere-se, ainda, aos padrões culturais de uma dada comunidade, atuando como uma *força anônima* incidente sobre as atitudes do profissional ao passo que os padrões legais, materializados na estrutura normativa de uma sociedade, visam a regular a dinâmica da mesma, mas muitas vezes, por conta de lacunas ou mesmo de excessiva regulamentação, podem ultrapassar os limites previstos e acabar prejudicando alguém.

A partir disso, Froehlich (1994, p. 463) chega a um conjunto de princípios condutores das ações éticas dos profissionais da informação: busca por justiça e harmonia social e, como consequência, a busca pela diminuição dos males, decorrência dos processos decisórios que os valores anteriores possam exigir.

Em seu *blog* denominado Laura´s Dark Archive, a bibliotecária inglesa Laura Wilkinson, ao abordar o papel das bibliotecas na proteção de dados (Wilkinson, s. f.), apresenta situações de dados pessoais com as quais uma biblioteca universitária, por exemplo, pode se deparar, como as informações pessoais dos usuários e funcionários, tais como nome, endereço, e-mail etc. Aliando-se a isso apresenta situações relativas a hábitos de consumo (caso haja uma loja virtual) e ainda informações sobre registros criminais, registros de emprego, etc.

Indo além apresenta princípios para o tratamento desses tipos de dados, de onde se destaca a imprescindibilidade de serem guardados somente para fins específicos, de forma não excessiva e em tempo não maior do que o necessário conforme as determinações legais e, por fim, serem mantidos em segurança e não serem transferidos, ainda que legalmente, a uma outra instância sem esta garanta adequado ou equivalente nível de proteção dos dados.

Por fim, apresenta um conjunto daquilo que se poderia denominar “dados sensíveis” e que somente podem ser arquivados com o explícito consentimento da(s) pessoa(s) envolvida(s), tais como origem racial ou étnica, preferências políticas, vinculação religiosa ou ideológica, saúde mental, vida sexual e outros.

4. Conclusão

Diante do contexto aqui exposto, observa-se que os dados pessoais se inserem cada vez mais em uma concepção produtivista e voltada à acumulação de riquezas, sendo não raras vezes expropriados de seus reais possuintes, sem o seu consentimento, e tratados e comercializados como uma commodity, para sua utilização como insumo para manufatura de informação e conhecimento, fonte de poder para a manutenção e reprodução do que Althusser (1980) preconiza como aparelho de Estado.

No caso brasileiro essa situação é particularmente preocupante em virtude da natureza dispersa e vaga da pouca legislação existente.

Isso leva a uma preocupação sobre o papel a ser desempenhado pelo profissional da informação, em especial no que tange a seu dever ético de proteção da privacidade de seus usuários, mais especialmente no que se refere aos dados pessoais. Nesse contexto, necessária se torna a constante investigação acerca de boas práticas e ferramentas para garantir tal privacidade e para reafirmar o papel social das unidades de informação.

Essa discussão confirma o estudo anteriormente realizado por Guimarães et. al (2008) quando se identificaram valores éticos diretamente ligados à prática do profissional da informação, mais especialmente no que se refere à organização e ao armazenamento da informação – e, obviamente, com consequências na disseminação dessa informação. Nesse sentido, observa-se o respeito à privacidade como o valor de maior incidência (20% dos casos estudados). Este valor, aliado ao da garantia pela segurança da informação e à minimização, corresponde a cerca de ¼ do total de valores, o que corrobora a hipótese aventada. Nesse mesmo trabalho, os autores elencam os problemas éticos incidentes nesse contexto, dentre os quais destacam-se a vigilância e à segregação digital que, juntos perfazem 29% do total de problemas éticos envolvidos.

Outro aspecto a ressaltar consiste em um maior envolvimento desse profissional, no caso do Brasil, com o disposto na Lei de Acesso à Informação (Lei 12527/2011), mais especificamente no que se refere à proteção da autenticidade e integridade da informação. Indo além, o texto legislativo, em seu artigo 31, refere-se ao "respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais".

No campo deontológico, observa-se que o artigo 11, alínea g do Código de Ética profissional do Bibliotecário (Resolução CFB 42/2002) refere-se textualmente à preservação das informações confidenciais, questão que envolve o sigilo profissional (previsto no artigo 12, alínea e).

Em uma tônica mais específica, os Princípios Éticos do Arquivista brasileiro (AAB, s.d.) estabelecem, em seus itens 1.7 e 1.9, o dever de assegurar a autenticidade e a integridade documental bem como respeitar a legislação em vigor em questões que envolvam sigilo, em especial no que tange à vida privada das pessoas. No campo das proibições, por sua vez, tem-se a vedação de divulgação de conteúdo de documentos de acesso restrito bem como qualquer invasão da privacidade dos usuários no que tange às pesquisas por eles empreendidas.

A vista do exposto, observa-se que a temática aqui discutida atinge diretamente os profissionais da informação em suas atividades de organização e de disseminação, atuando como importante promotores da proteção de dados pessoais.

Referencias

Associação dos Arquivistas Brasileiros. Princípios éticos do Arquivista. Rio de Janeiro: AAB, s.d. http://portal.tcu.gov.br (2019-06-01).

Acquisti, Alessandro (2013). The economics of privacy: theoretical and empirical aspects. New York: Center for Urban Science and Progress, 2013. http://cusp.nyu.edu/wp-content/uploads/2013/09/C03-acquisti-chapter.pdf (2017-2-04).

Althusser, Louis (1980). Ideologia e aparelhos ideológicos do Estado. 3ª ed. Lisboa: Presença, 1980.

Araújo, Carlos Alberto Ávila (2010). O conceito de informação na Ciência da Informação. Informação & Sociedade. ISSN 1809-4783. 3:20 (dezembro 2010) 95-105.

Bacellar Filho, Romeu Felipe; Schier, Adriana da Costa Ricardo (2013). Direito à informação e a aplicação da Lei nº 12.527/11 às organizações sociais. // Bacellar filho, Romeu Felipe; Hachem, Daniel Wunder (coord.). Direito Público no Mercosul: intervenção estatal, direitos fundamentais e sustentabilidade. Belo Horizonte: Fórum, 2013.

Banisar, David (2017). National comprehensive data protection/privacy laws and bills 2016. https://ssrn.com/abstract=1951416 (2017-3-02).

Barreto, Aldo Albuquerque (2000). O mercado de informação no Brasil. Informação & Informação. ISSN 1981-8920. 1:5 (junho 2000) 25-34.

Bauman, Zygmunt; Lyon, David (2014). Vigilância Líquida. 1ª ed. Rio de Janeiro: Zahar, 2014. ISBN 8537811564.

Brasil (2016). Câmara dos Deputados: Projeto de Lei nº 5276 de 13 de maio de 2016. http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378 (2017-02-14)

Brasil. Congresso Nacional. Lei nº 12.527 de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e da outras providências. // Diário Oficial da União, Poder Executivo, Brasilia, DF, 18 nov. 2011 – edição extra. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm (2018-27-02).

Capurro, Rafael.; Hjorland, Birger (2007). O conceito de informação. Perspectivas em Ciência da Informação. ISSN 1981-5344. 12:1 (abril 2007) 148-207.

Carraretto, André (2014). A onda dos "mega" vazamentos de dados. https://canaltech.com.br/seguranca/A-onda-dos-mega-vazamentos-de-dados/. 2017-02-09.

CFB. Conselho Federal de Biblioteconomia. Resolução 42/2002. http://repositorio.cfb.org.br/handle/123456789/1101 (2018-27-02).

Creativante (2014). Data brokets (corretores de dados). http://www.creativante.com/new/index.php/2013-02-03-19-36-05/2014/212-data-brokers-corretores-de-dados (2017-01-19).

Doneda, Danilo (2011). A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico. ISSN 2179-7943. 2:12. (dezembro 2011) 91-108.

ESET (2016). ESET Security Report Latinoamérica 2016. https://www.welivesecurity.com/wp-content/uploads/2016/04/eset-security-report-latam-2016.pd. (2017-07-06)

Fortes, Vinícius Borges; Boff, Salete Oro (2014). A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil. Sequência: Estudos Jurídicos. ISSN 2177-7055. 35:68 (junho 2014) 109-128.

Gil-Leiva, Isidoro; Moya, Gregorio Martínez (2011). El acceso a la información pública: estúdio de casos de Brasil, España y Portugal. // Informação & Sociedade. ISSN 1809-4783. 21:1 (abril 2011) 73-89.

Guimarães, J. A. C. (2008). O profissional da informação sob o prisma de sua formação. // Valentim, M. L. P. Profissionais da informação: formação e atuação profissional. São Paulo: Polis, 2008. 57-70.

Guimarães, J. A. C; Sales, R. (2010). Análise documental: concepções do universo acadêmico brasileiro em Ciência da Informação. Datagramazero. ISSN 1981-0695. 11:02 (fevereiro 2010) 02.

Guimarães, J. A. C.; Pinho, F. A.; Milani, S. de O.; Fernandez-Molina, J. C. (2008). Ética nas atividades informativas: aspectos teóricos. PontodeAcesso. ISSN 1981-6766. 02:01 (julho 2008) 138-153.

Lima, Caio Cesar Carvalho; Monteiro, Renato Leite (2013). Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada. Atoz. ISSN 2237-826X. 01:02 (janeiro 2013) 60-76.

Novaes, Rafael (2014). Conheça as data brokers: empresas que coletam suas informações. http://www.psafe.com/blog/conheca-data-brokers-empresas-coletam-suas-informacoes (2017-01-19).

Otlet, P. (1934). Traité de documentation: le livre sur le livre: théorie et pratique. Bruxelles: Mundaneum, 1934.

Pariser, Eli (2012). O filtro invisível: o que a internet está escondendo de você. 1ª ed. Rio de Janeiro: Zahar, 2012. ISBN 8537808032.

Pinheiro, Lêna Vânia Ribeiro (2005). Processo evolutivo e tendências contemporâneas da Ciência da Informação. Informação & Sociedade. ISSN 1809-4783. 1:15 (junho 2005) 13-48.

Pomart, P. D.; Sutter, D (2004). Valeur de l´information. // Cacaly, Y.; et al. Dictionnaire de l´information. 2ª ed. Paris: Armand Colin, 2004. ISBN 2200266820.

Rocha, Isadora Martins Marques da; Konrad, Glaucia Vieira Ramos (2013). A conduta do arquivista frente à Lei de Acesso à Informação. Informação Arquivística. ISSN 2316-7300. 02:02 (dezembro 2013) 103-123.

Sá, A. L (2009). Ética profissional. 9ª ed. São Paulo: Atlas, 2009. ISBN 8522455341.

Santos, João Carlos Gardini (2016). As dimensões teóricas da informação na jurisprudência brasileira: uma análise a partir dos acórdãos do Supremo Tribual Federal. Marília: FAPESP, relatório nº 3, processo nº 2015/05761-5.

Semidão, Rafael Aparecido Moron (2014). Dados, informação e conhecimento enquanto elementos de compreensão do universo conceitual da Ciência da Informação: contribuições teóricas. Marília; Universidade Estadual Paulista, 2014. Tesina.

Serasa Experian (2014). Mosaic. O poder da segmentação de clientes ao seu alcance. https://marketing.serasaexperian.com.br/targeting/mosaic/. 2017-03-02.

Silva, Naiara Bárbara Xavier; Araújo, Wagner Junqueira de; Azevedo, Patrícia Morais de (2013). Engenharia social nas redes sociais online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. // Revista Iberoamericana de Ciência da Informação. ISSN 1983-5213. 02:06 (dezembro 2013) 37-55.

Silveira, Sergio Amadeu; Avelino, Rodolfo; Souza, Joyce (2016). A privacidade e o mercado de dados pessoais. // Liinc. ISSN 1808-3536. 12:02 (novembro 2016) 217-230.

Smit, J. W.; Barreto, A. A (2002). Ciência da Informação: base conceitual para a formação do profissional. // Valentim, M. L. P. (org.). Formação do profissional da informação. São Paulo: Polis, 2002. ISBN 85-7228-014.

Smit. J. W. O que é documentação (1986). 2ª ed. São Paulo: Brasiliense, 1986. ISBN 85-11-01174-9.

Washington, Federal Trade Commission (2017). Data Brokers: A Call For Transparency and Accountability 2014. https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014 (2017-03-02).

Wecker, John; Adeney, Douglas (2000). Ética informática y de las Ciencias de la Información. 1ª ed. Madrid: Editorial Fragua, 2000. ISBN: 84-7074-115-2

Wilkinson, Laura. Laura´s Dark Archive. https://darkarchive.wordpress.com/2012/03/01/libraries-and-the-data-protection-act/ (06.04.2018).

Xavier, R. C. M.; Costa, R. O. (2010). Relações mútuas entre informação e conhecimento: o mesmo conceito? // Ciência da Informação. ISSN 1518-8353. 39:02 (agosto 2010) 75-83.

Enviado: 2018-04-24-. Aceptado: 2018-06-05.