



OS DADOS PESSOAIS E A PROTEÇÃO DE DADOS DE SAÚDE: ANÁLISE A PARTIR DAS INICIATIVAS DE e-SAÚDE

PERSONAL DATA AND MEDICAL DATA PROTECTION: AN ANALYSIS UNDER e-HEALTH INITIATIVES

Letícia Seibel Siqueira ¹
Patrícia Adriani Hoch ²

RESUMO

Diante da ampla utilização das tecnologias de informação e comunicação (TIC), dados pessoais dos indivíduos são armazenados em bancos informatizados e interconectados, a exemplo das iniciativas e-Saúde. Nesse contexto, destacam-se as inúmeras formas de violação a direitos fundamentais, como o direito à privacidade do paciente, razão pela qual a proteção de dados pessoais revela-se um tema relevante a ser abordado e discutido. Assim sendo, o objetivo deste trabalho consiste em compreender o nível de proteção conferido aos dados pessoais, em especial os de saúde, no âmbito das novas tecnologias, nas quais estão inseridas as iniciativas de e-Saúde. Para tanto, o método de abordagem utilizado foi o dedutivo, visto que a pesquisa partiu de uma análise geral sobre a proteção da privacidade e do tratamento de dados de saúde, realizando, em seguida, um estudo dos possíveis benefícios, riscos e desafios à garantia da privacidade dos pacientes no uso de suas informações por meio das novas tecnologias. Utilizou-se, ainda, o método de procedimento comparativo, bem como as técnicas de pesquisa documental e bibliográfica. Constatou-se que o Brasil, ainda que tardiamente frente aos avanços mundiais, iniciou produção legislativa, que entrará em vigor em 2020, que garante guarida aos dados pessoais. Ainda, a produção técnica jurídica deve estar alinhada ao conceito dinâmico e atual de tutela da privacidade, coadunando-se com as evoluções informáticas na área da segurança e da proteção dos dados pessoais, especialmente os sensíveis, como os de saúde.

Palavras-chave: Dados pessoais; Direito à privacidade do paciente; Iniciativas de e-Saúde; Tecnologias de Informação e de Comunicação;

ABSTRACT

Due to the massive use of information and communication technologies (ICT), individual's personal data are stored in computerized and interconnected databases, such as e-Health initiatives. From this context, several forms of violation to human rights, like patient's right to privacy, are highlighted. Therefore, personal data protection appears an interesting issue to be approached and debated. For this reason, the purpose of this study is to understand the level of protection given to personal health data in the context of new technologies, where e-Health initiatives are inserted. To this end, the deductive approach was used, considering that the research started from a general analysis about privacy protection and medical data treatment. Then, it was carried out a study of the benefits, risks and challenges to patient's privacy guarantee in the use of their information by

¹ Pós-Graduada em Relações Internacionais, com ênfase em Direito Internacional da Faculdade de Direito Damásio de Jesus. Graduada em Direito pela UFSM. Integrante do NUJUDI (Núcleo Jurisdição Constitucional e Direitos Fundamentais). Advogada. lseibelsiqueira@gmail.com

² Doutoranda em Direito Público pela UNISINOS. Mestre em Direito pela UFSM. Pós-graduada em Direito Processual Tributário pela Anhanguera. Professora do Curso de Direito da UFSM e Coordenadora do NUJUDI. Advogada. patricia.adriani@hotmail.com



new technologies. The work was also performed by using the comparative procedure as well as by applying bibliographic and documentary research techniques. The results showed that although Brazil is delayed in regard to worldwide advances, it has started legislative regulation which will come up in 2020 and will guarantee protection to personal data as well. Thus, legal production must be aligned with current and dynamic concept of privacy protection, being in conformity with computer evolutions in the field of security and personal data, especially the sensitive ones, like health data.

Keywords: Personal data; Patient's right to privacy; e-Health initiatives; Information and Communication Technologies.

INTRODUÇÃO

No Século XXI evidencia-se, em larga escala, a utilização de novas tecnologias, computadores e Internet, com a crescente estruturação da sociedade em rede, conceituada há muito por Manuel Castells. Nessa perspectiva, ocorre a sedimentação, em grande volume, das informações em bancos de dados informatizados e interconectados, em todos os níveis, seja pelo Poder Público ou pela iniciativa privada.

Por consequência, esse contexto tecnológico, aliado ao armazenamento e difusão de informações, alerta para a necessidade de melhor compreensão do papel jurídico a ser exercido frente à utilização das tecnologias de informação e de comunicação (TIC). Isso, pois, no âmbito informacional, não raro direitos fundamentais, como a privacidade e a intimidade do indivíduo, são violados, sendo imprescindível a reflexão a respeito da eficácia desses direitos tutelados em legislação pátria e internacional.

O uso indevido e o acesso desenfreado aos dados de caráter pessoal são atentatórios e banalizam o direito à privacidade do indivíduo, na medida em que, não raras vezes, esse desconhece totalmente o destino que será atribuído aos seus registros. O Brasil, ainda que tardiamente, instituiu lei específica de proteção dos dados pessoais de seus cidadãos, no ano de 2018 (Lei nº 13.709), a qual foi intitulada como a Lei Geral de Proteção de Dados Pessoais (LGPD) e ainda não entrou plenamente em vigor.

Conforme prevê o artigo 5º, inciso II, da referida lei, importantes e sensíveis ramificações dos dados pessoais são os dados de saúde, também chamados de dados clínicos ou, simplesmente, de informações médicas. O alto potencial discriminatório e lesivo de tais dados é o que impulsiona a imprescindibilidade de sua proteção e preservação, como forma de garantir o direito à dignidade, ao sigilo e à vida privada de seus titulares. Ademais, o meio digital está despontando como primário eleito para o



processamento, tratamento e armazenamento dos dados de saúde, especialmente por meio da perspectiva da e-Saúde e dos bancos de dados informatizados.

Partindo-se dessas premissas, o presente estudo visa à compreensão da proteção conferida aos dados de saúde, diante da tutela de dados pessoais, a partir da utilização das tecnologias de informação e de comunicação (TIC), especialmente da Internet, bem como das iniciativas de e-Saúde. Objetiva-se investigar os benefícios e possíveis riscos e possibilidades de ofensa à intimidade e à vida privada dos pacientes no uso de tais tecnologias e no manejo dos dados de saúde.

Para tanto, foi utilizado o método de abordagem dedutivo, aliado à aplicação de técnicas de pesquisa documental e bibliográfica, partindo-se da temática da proteção dos dados pessoais, com ênfase para dados de saúde, e respeito à vida privada dos pacientes, tendo como base a produção normativa nacional e internacional existente a respeito do tema, para o estudo das iniciativas de e-Saúde. Ademais, elegeu-se o método de procedimento comparativo, expondo-se a atual lei brasileira de proteção de dados em relação às anteriores, de outros países, que serviram de inspiração para a produção nacional.

Para a fluidez da compreensão, o artigo foi dividido em duas partes: na primeira, tratar-se-á do direito humano fundamental do respeito à vida privada do paciente, sobretudo quanto à proteção dos dados de saúde. A partir disso, no segundo tópico será realizada a reflexão crítica a respeito da tutela dos dados de saúde dos pacientes em face do fenômeno da e-Saúde.

1 OS DADOS DE SAÚDE E O RESPEITO À VIDA PRIVADA DOS PACIENTES

A sociabilidade humana enfrenta um fenômeno similar à ocorrência natural de um furacão, ao assistir a movimentos na superfície que deslocam os seres sociais da presença à ausência, e a morfologia social do físico ao digital. O sociólogo espanhol Manuel Castells afirma surgir, assim, a Sociedade em Rede, na qual “as bases significativas da sociedade, espaço e tempo estão sendo transformadas, organizadas em torno do espaço de fluxos e do



tempo intemporal”³. A integração em rede, segundo o autor, “[...] tornou-se aplicável a todos os tipos de atividade, a todos os contextos e a todos os locais que pudessem ser conectados eletronicamente”⁴.

A evolução tecnológica, o uso massivo e crescente dos computadores, e o surgimento da internet e das tecnologias de informação e comunicação (TIC), em meados da década de 70 do século passado, foram contemporâneos às primeiras reflexões jurídicas e consequentes legislações existentes sobre o tema da proteção dos dados pessoais. Atualmente, cerca de 120 países - incluindo múltiplos Estados latino-americanos -, norteados pelas normativas europeias, já editaram legislação específica de proteção dos dados pessoais, em clara percepção dos riscos inerentes à ampla disseminação e ao tratamento desenfreado das informações de caráter privado.

Os países integrantes da União Europeia, pioneiros na tutela estatal do tema, inauguraram suas preocupações com a temática em 1970, com uma lei, editada pelo Estado alemão de Hesse, que se preocupava com o manejo mecânico dos dados pela administração pública. Desde então, os europeus atribuem amplo respeito à proteção e à privacidade dos dados pessoais, garantidos por meio de uma sólida normatização, atualmente expressa no Regulamento nº 2016/679 do Parlamento Europeu e do Conselho⁵.

O Brasil, por outro lado, apresenta-se em um patamar inferior, haja vista que, somente no ano de 2018 editou lei específica para a segurança dos dados pessoais de seus cidadãos. A Lei Geral de Proteção de Dados Pessoais (LGPD ou LGPDP), Lei nº 13.709/2018⁶, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet. Expressa lei,

³ CASTELLS, Manuel. **A sociedade em rede** - a era da informação: economia, sociedade e cultura. 5. ed. Traduzido por Klauss Brandini Gerhardt e Roneide Vanancio Majer. São Paulo: Paz e Terra, 1999, p. 572.

⁴ *Ibidem*, p. 89.

⁵ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, L 119, p. 1 - 88. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT>>. Acesso em: 19 jun. 2019.

⁶ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 jun. 2019.



publicada em 14 de agosto de 2018, somente entrará em vigor plenamente no ano de 2020, em decorrência da *vacatio legis* prevista em seu texto.

O ordenamento pátrio apresentou, até o advento da LGPD, somente nuances e algumas previsões sobre a temática em legislações como o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e a Lei do *Habeas Data* (Lei nº 9.507, de 12 de novembro de 1997), além de disposições gerais sobre privacidade encontradas na Constituição Federal e em outras leis esparsas. Afirma-se, portanto, que, no Brasil, até então, não havia proteção aos dados pessoais integrada e alinhada aos comandos constitucionais, mas sim atuações fracionadas em focos específicos, a exemplo da tutela exercida no Código de Ética Médica.

O emprego de *softwares*, equipamentos e computadores para o tratamento de dados pessoais, o processamento desses de maneira intensa, além da criação de bancos ou bases de dados, elevaram a importância da informação pessoal a tal patamar que ela passou a se tornar o núcleo principal da temática da privacidade e intimidade. Por consequência, foi desintegrado o seu conceito clássico diante dessas atualizações, impondo-se contornos próprios e dando-se continuidade à sua disciplina. Segundo dicção do doutrinador Danilo Doneda:

A informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encerra toda a complexa problemática em torno dessa relação, porém pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela do direito à privacidade.⁷

Assim, o desenvolvimento das tecnologias informacionais e a sucessiva ressignificação do conceito de proteção da privacidade, como além do direito de ser deixado ou de estar só - “*right to be alone*”⁸ -, também o direito de manter controle sobre

⁷ DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, v. 12, p. 91-108, 2011. Disponível em: <<http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658>>. Acesso em: 30 jun. 2019.

⁸ Esse conceito e construção jurídica surgiu, originalmente, em um artigo publicado por dois juristas norte-americanos, Samuel D. Warren e Louis D. Brandeis, na *Harvard Law Review*, intitulado *The Right to Privacy*. BRANDEIS, Louis D.; WARREN, Samuel D. *The Right to Privacy*. *Harvard Law*



as próprias informações, atualizando-o para uma proteção específica do tratamento autônomo dos dados pessoais, demandou dos países novos perfis jurisprudenciais e legislativos.

O Autor espanhol Perez Luño⁹, ao constatar a importância da intimidade no contexto atual, esclarece que a honra, intimidade e a imagem constituem direitos da personalidade, como expressões do valor da dignidade humana, o qual é tutelado na Constituição Federal brasileira. É neste sentido que, pertencendo à categoria dos direitos fundamentais, a violação da intimidade através da utilização de ferramentas eletrônicas merece especial atenção. Além disso, o Autor salienta que o direito à intimidade pode ser entendido sob dois aspectos: o primeiro é o negativo, que trata do direito do indivíduo a não ser molestado; já o segundo é positivo e relaciona-se com uma atitude mais ativa dos cidadãos no que concerne à coleta e à utilização de seus dados.

Um desdobramento do direito à intimidade consiste no princípio ou direito da autodeterminação informativa, inserto na atual legislação pátria de proteção dos dados pessoais, o qual diz respeito ao “[...] direito de a pessoa decidir quando e como está disposta a permitir que seja divulgada a sua informação pessoal, ou a difundi-la por vontade própria”¹⁰. O direito à autodeterminação informativa surgiu a partir de uma decisão proferida em 1983 pelo Tribunal Constitucional da Alemanha, que declarou parcialmente inconstitucional lei que obrigava os cidadãos a responderem as perguntas do censo populacional para formação posterior de um banco de dados. Logo, a ideia intrínseca à efetivação da autodeterminação informativa consiste na possibilidade de que o titular dos dados forneça consentimento prévio para que terceiros façam o uso das informações pessoais.

Os ordenamentos jurídicos comunitários e nacionais dos Estados integrantes da União Europeia foram vanguardistas, portanto, na reformulação das leis de proteção das informações de caráter pessoal, a partir do novo enfoque formulado para o tópico da privacidade e intimidade, seguidos por ordenamentos nacionais de múltiplos países não europeus. O advento do sistema protetivo criado para as bases de dados e para as

Review, v. IV, 1980. Disponível em: <http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html>. Acesso em: 16 jun. 2019.

⁹ LUÑO, Antonio Enrique Perez. *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Editorial Tecnos, 2005.

¹⁰ LIMBERGER, Temis. *O direito na era da informática: a necessidade de proteção dos dados pessoais*. Porto Alegre: Livraria do Advogado, 2007, p. 103.



informações de caráter pessoal, em escala mundial, é fruto do direito geral de personalidade, dentro do qual está inserido o direito à vida privada.

Após essa breve contextualização do panorama geral da proteção dos dados pessoais, esse trabalho volta-se ao seu objeto de estudo original, com a subdivisão específica de tal categoria: os dados de saúde. As informações de saúde, ou, simplesmente, informações médicas, enquadram-se no subgrupo conhecido como de caráter sensível, conforme previsão contida no artigo 5º, inciso II, da Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira¹¹.

São rotuladas como informações sensíveis dos cidadãos as que apresentam alto potencial discriminatório ou recriminatório ao seu titular, ostentando maiores riscos que a média para o indivíduo e, até mesmo, para a coletividade¹². Devido ao elevado grau de lesividade dos dados sensíveis, em razão de revelarem informações de cunho personalíssimo, enraizadas na esfera de proteção do direito de personalidade, sua coleta, processamento e tratamento devem ocorrer somente após a anuência e o consentimento expresso do titular, pois, fato contrário, estar-se-ia violando a esfera do segredo, das confidências e reservas do ser.

São tidos como dados sensíveis, entre outros, aqueles que desvelam a origem racial ou étnica do titular, os seus princípios políticos, morais, filosóficos ou religiosos, filiações partidárias ou sindicais, antecedentes criminais, orientações sexuais, além, é claro, dos dados médicos e de saúde. Muitos formulários, preenchidos fisicamente ou *online*, contêm informações personalíssimas do indivíduo, sobretudo quanto à orientação sexual ou doença grave, razão pelas quais a proteção desses dados deve ser segura e adequada. “Um portador do vírus HIV (vírus da Imunodeficiência Humana) pode não ser contratado por uma

¹¹ “II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 jun. 2019.

¹² SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <<http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>>. Acesso em: 21 jun. 2019.



empresa, em virtude da doença, o que caracterizaria uma situação de desigualdade”¹³. A prejudicialidade do uso de informações captadas por bancos de dados, especialmente quando referentes à religião, sexo ou saúde, é alertada por Temis Limberger¹⁴.

Há construção teórica e legislativa, no plano internacional, que fomenta a utilização do referencial de “direitos humanos dos pacientes” (DHP), previstos em documentos elaborados e adotados no âmbito de organizações e sistemas internacionais, como ferramenta para análise de imbrólios éticos que exsurtem na área da saúde¹⁵.

São considerados direitos humanos aplicáveis ao contexto dos cuidados em saúde e de pacientes o direito à vida, o direito a não ser submetido a tratamento desumano, degradante, cruel ou à tortura, o direito à liberdade e segurança pessoal, o direito à saúde integral, o direito de não sofrer discriminação de qualquer tipo, e, especialmente relevante ao presente propósito, o direito à informação e ao respeito à vida privada.

Pode-se afirmar, assim, a partir da abordagem exposta, que os dados médicos revelam-se como importante ramificação dos dados pessoais e consistem em informações sensíveis de saúde depositadas em hospitais, após internações ou cirurgias, em laboratórios, após a coleta de exames, em clínicas, após a realização de procedimentos, em consultórios médicos, odontológicos, fisioterapêuticos, psicológicos ou psiquiátricos, após a realização de consultas e sessões, ou até mesmo em cadastros de planos de saúde, após a solicitação de autorização para realização de exames ou procedimentos. Além dos dados de saúde, os registros dos pacientes em citados estabelecimentos contêm inúmeras informações de cunho pessoal, incluindo nomes, datas de nascimento, endereços, números de seguro e de planos de saúde de cada indivíduo.

Frisa-se, como será mais bem explicitado no segundo capítulo deste trabalho, que o depósito de tais dados, na atual sociedade informacional que presenciamos, ocorre sobremaneira no meio digital. Ainda, que o processamento e a transmissão dos dados médicos podem variar entre a simples comunicação de casos entre profissionais da saúde

¹³ HOCH, Patrícia Adriani. **Levando a intimidade a sério no contexto da sociedade em rede**. Dissertação (mestrado). Universidade Federal de Santa Maria, 2017, p. 38.

¹⁴ LIMBERGER, Temis. **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais**. Porto Alegre: Livraria do Advogado, 2007, p. 218-219.

¹⁵ PARANHOS, Denise G.A.M.; ALBUQUERQUE, Aline. Direitos humanos dos pacientes como instrumentos bioéticos de proteção das pessoas idosas. **Cadernos Ibero-Americanos de Direito Sanitário**, Brasília, v. 8, n.1, p. 53-64, 2019. Disponível em: <<https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/issue/view/30/showToc>>. Acesso em: 18 jun. 2019.



de um estabelecimento hospitalar, até o compartilhamento mais complexo de informações entre instituições de atenção à saúde, por meio de bancos de dados, por exemplo, transmitidos pela rede local ou via *Internet*.¹⁶

Ainda que compreensível no plano teórico, a imprescindibilidade de proteção dos dados pessoais dos pacientes e dos usuários dos sistemas de saúde verifica-se pouco factível no plano prático, haja vista que, no contexto brasileiro, o armazenamento e o posterior uso dos dados médicos revestem-se de certa obscuridade. Isso, pois, não é proporcionado o dimensionamento correto, ao usuário, quanto a potencial lesividade ao direito fundamental humano da privacidade em caso de possíveis vazamentos ou acessos indevidos.

Os Estados Unidos da América, já no longínquo ano de 1973, divulgou um estudo, editado por uma comissão de especialistas reunida pela *Secretary for health, education and welfare*. A área da saúde foi pioneira na demonstração de justificado receio com a manipulação de dados médicos por sistemas informatizados, ao passo que referida pesquisa igualmente concluiu pelo estabelecimento de relação direta entre o tratamento de dados e o direito de privacidade, além da criação de necessárias normas para o exercício de controle, pelo indivíduo, sobre a posterior divulgação e utilização de suas informações:

A privacidade pessoal de um indivíduo é afetada diretamente pelo tipo de divulgação e utilização que é feita das informações registradas a seu respeito. Um tal registro, contendo informações sobre um indivíduo identificável deve, portanto, ser administrado com procedimentos que permitam a este indivíduo ter o direito de participar na sua decisão sobre qual deve ser o conteúdo deste registro e qual a divulgação e utilização a ser feita das informações pessoais nele contida. Qualquer registro, divulgação e utilização das informações pessoais fora destes procedimentos não devem ser permitidas, por consistirem em uma prática desleal, a não ser que tal registro, utilização ou divulgação sejam autorizados por lei¹⁷. (tradução nossa)

¹⁶ KAMEDA, Koichi; PAZELLO, Magaly. E-Saúde e desafios à proteção da privacidade no Brasil. *PoliTICs*, v. 16, p. 31-40, 2013. Disponível em: <<https://politics.org.br/edicoes/esa%C3%BAedesa%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil>>. Acesso em: 20 jun. 2019.

¹⁷ “An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law.” ESTADOS UNIDOS DA AMÉRICA. *Records, computers and the rights of citizens*. Report of the Secretary's Advisory



Nessa perspectiva, diante dos múltiplos atores que demonstram interesse e cercam os dados de saúde da população, a exemplo de empresas seguradoras, planos de saúde, laboratórios, *hackers* e estelionatários, e, até mesmo diante dos riscos inerentes a fragilidade das informações médicas, a participação do indivíduo no seu processamento deve ter início a partir da coleta de seus dados.

A autodeterminação informativa do paciente, que é fundamento da LGPD e deve ser protegida com base no disposto no artigo 2º, inciso II, inaugura-se com o preenchimento do termo de consentimento esclarecido e informado, documento necessário tanto para a realização de intervenções cirúrgicas ou procedimentos, como para a prática de pesquisa, fatos que desencadeiam, por si só, a colheita de dados de saúde do indivíduo. Os termos de consentimento devem conter avisos claros relativos ao grau de confiabilidade de exames, alertas de possíveis riscos, consequências fisiológicas e complicações, além do caráter, objetivos e benefícios da intervenção. O termo deve estar escrito em linguagem simples e decodificada do jargão médico ou científico, de forma que o paciente esteja livre e plenamente consciente do teor da sua permissão.

Escassos são os termos de consentimento, entretanto, que alertam o paciente quanto aos possíveis usos, destino e armazenamento a que serão submetidos os seus dados de saúde. Alerta-se, desse modo, para os riscos e ameaças veladas ao direito de privacidade e intimidade do indivíduo, que acabam sendo legitimados a partir de sua assinatura em documentos que buscam o consentimento:

[...] o que se tem verificado, em alguns momentos, é a habilidade e o esforço dissimulador da intenção abusiva, escamoteada tantas vezes por motivações “justas” e “necessárias”. A licitude de um ato dessa natureza não está só no consentimento, mas na sua necessidade e na sua legitimidade. Assim, mesmo que a permissão tenha todas as aparências e justificativas de idoneidade, e mesmo que exista aquiescência por escrito, chega-se à conclusão que a vida e a saúde de um indivíduo são bens irrecusáveis e inalienáveis, os quais o bem comum tem interesse em resguardar de forma irrestrita e incondicional. As ciências necessitam mais e mais progredir. Algumas vezes até pela ousadia de suas intercessões, de resultados tão fantásticos e inesperados. Todavia, isso não justifica a

Committee on Automated Personal Data Systems. 07 de janeiro de 1973. Disponível em: <<https://aspe.hhs.gov/report/records-computers-and-rights-citizens>>. Acesso em: 21 jun. 2019.



violência sobre um só homem, qualquer que seja sua condição, qualquer que seja o progresso pretendido.¹⁸

Os termos de uso ou políticas de privacidade, especialmente quanto aos dados de pacientes depositados na *Internet*, são ou inexistentes ou inadequados, muitas vezes escritos em língua estrangeira, e em caracteres pequenos que dificultam a leitura. Tais fatos cerceiam a informação e a precisão da trajetória que será percorrida pelas informações médicas do cidadão, desde sua coleta até posterior armazenamento e destino final.

Reconhece-se que não há, portanto, clareza quanto ao tratamento que será efetivado aos dados pessoais e de saúde dos pacientes e dos usuários do sistema de saúde brasileiro, conjuntura atentatória ao seu direito de informação, ao princípio da autodeterminação informativa e ao direito à privacidade do paciente.

2 O PRONTUÁRIO ELETRÔNICO E AS INICIATIVAS DE E-SAÚDE

O filósofo e sociólogo Zygmunt Bauman analisou o tema da vigilância, ao qual conferiu status de dimensão central da modernidade, e assim o fez por meio do conceito de liquidez, nomeando-o de “vigilância líquida”¹⁹. Tal definição faz referência ao fato da vigilância ter se tornado mais móvel e flexível, infiltrando-se em áreas até então desconhecidas, imbricadas no foro íntimo das pessoas. O autor, ao discorrer sobre a noção de vigilância líquida, alerta sobre a forma como “[...] dados do corpo (dados biométricos, DNA) [...] são sugados para bases de dados a fim de serem processados, analisados, concatenados com outros dados e depois cuspidos de volta como “replicação de dados”²⁰.

Ou seja, todo tratamento e processo conferido aos dados pessoais de uma pessoa, especialmente os de saúde, que são aqueles que se originam em seu corpo, conduzem à categorização desse indivíduo, influenciando em suas escolhas e oportunidades existenciais. Visualiza-se, assim, que “[...] a “replicação e fragmentação de dados” tende a inspirar mais confiança que a própria pessoa - que prefere contar sua própria história”²¹.

¹⁸ FRANÇA, Genival Veloso de. **Direito médico**. 14. ed. rev. e atual. Rio de Janeiro: Forense, 2017.

¹⁹ BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. 1. ed. Traduzido por Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

²⁰ Ibidem, p. 15.

²¹ Ibidem, p. 15.



A vigilância já aterrissou na Internet e nos dados pessoais e de saúde lá armazenados. O progresso na capacidade de transmissão de informações, a expansão do acesso ao conhecimento, o próprio surgimento da internet e a decorrente criação de espaços sociais virtuais foram elementos que penetraram nos poros visíveis da área da saúde e que, combinados, modificaram a estrutura operacional do setor, a maneira de armazenar e tratar os dados médicos e a consequente reflexão jurídica sobre o assunto.

A expressão e-Saúde, acolhida pela Organização Mundial da Saúde (OMS), e comumente denominada como telessaúde ou telemedicina, existe para designar as atividades, no campo da atenção à saúde, que fazem uso das Tecnologias de Informação e Comunicação (TIC), a fim de aprimorar e proporcionar alta qualidade de atendimento médico à população. São consideradas práticas de e-Saúde o teleatendimento, o telediagnóstico, os prontuários digitais, os bancos de dados médicos informatizados, as teleconsultorias, as videoconferências, as telecirurgias, a tele-educação, as bibliotecas virtuais de vídeos e imagens, o desempenho de segundas opiniões formativas, dentre inúmeros outros exemplos²².

No Brasil, a prática da e-Saúde encontra-se em estado de ascensão. Em rápida busca na Internet, encontram-se diversas iniciativas que utilizam a tecnologia integrada aos serviços de saúde. Como exemplo, cita-se o Programa Nacional de Telessaúde, parte integrante do Sistema Único de Saúde (SUS), que preza pela ampliação da resolutividade da Atenção Básica, a Rede Universitária de Telemedicina (RUTE), criada pelo governo federal com o propósito de unir faculdades de medicina e hospitais universitários de diferentes regiões do território brasileiro, o aplicativo “e-Saúde”, do Ministério da Saúde, que armazena dados dos usuários do SUS²³, além, por certo, da adoção do prontuário eletrônico por consultórios privados, hospitais e pelo sistema público de saúde.

Sucessivamente, os prontuários físicos, arquivados em pastas e escritos à mão pelos profissionais de saúde, estão sendo substituídos por aplicativos e sistemas eletrônicos de arquivos digitais. Assim, a problemática da necessidade de grande espaço físico para

²² REZENDE, Edson José Carpintero, et al. Ética e Telessaúde: reflexões para uma prática segura. *Panam Salud Publica*, v. 28, p. 58-65, 2010. Disponível em: <https://scielosp.org/scielo.php?pid=S1020-49892010000700009&script=sci_abstract&tlng=pt>. Acesso em: 28 jun. 2019.

²³ BRASIL. Governo Federal. *Aplicativo vai ampliar o acesso da população às informações de saúde*. 2017. Disponível em <<http://www.brasil.gov.br/saude/2017/06/aplicativo-vai-ampliar-o-acesso-da-populacao-as-informacoes-de-saude>>. Acesso em 30 jun. 2019.



armazenar prontuários “de papel” foi solucionada com o desenvolvimento de alternativas para arquivar os dados de saúde, por meio de *softwares* e programas de prontuário eletrônico.

Já há, inclusive, cartilha do Conselho Federal de Medicina (CFM), em parceria com a Sociedade Brasileira de Informática em Saúde (SBIS), lançada em 2012, que orienta os profissionais acerca da necessidade de certificação dos sistemas de registro eletrônico de saúde, como forma de garantir a segurança e a confidencialidade para as informações do paciente. A cartilha orienta o uso de mecanismos correlacionados, segurança de rede, criptografia de dados, monitoramento de acesso e assinaturas digitais, simultaneamente às certificações de segurança, como forma de tornar mais concreta a privacidade dos dados pessoais dos usuários²⁴.

O CFM, da mesma forma, aprovou resolução em 2007 que dispõe sobre normas técnicas atinentes à digitalização e ao uso de sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes no qual atesta ser o próprio paciente o titular do prontuário²⁵. Percebe-se, assim, que as normativas técnicas e setoriais sempre foram vanguardistas na elaboração de legislações que protegessem a privacidade dos dados pessoais dos cidadãos. Ainda assim, fato recente, noticiado pela imprensa, que divulgou o vazamento de informações de saúde que estavam inseridas no aplicativo do SUS²⁶, comprova a fragilidade e a vulnerabilidade a que estão submetidos os dados expostos em bancos digitais, no Brasil.

De todo modo, não se pode divulgar apenas as mazelas da inovação, pois a exploração de dados e a utilização das TIC não são sinônimos fiéis de um panorama negativo. Pesquisadores da área da saúde são enfáticos ao proferir que as tecnologias da

²⁴ BORROZZINO, Nélio Fernandes; PIZA, Ivan Torres. Aspectos legais do Prontuário Eletrônico do Paciente: Um Comparativo do Cenário Atual Frente a Resolução do CFM. *Ciência et Praxis*, Belo Horizonte, v. 8, n.15, p. 23-27, 2015. Disponível em: <<http://revista.uemg.br/index.php/praxys/article/view/2150/1142>>. Acesso em: 18 jun. 2019.

²⁵ CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.821/2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. *Diário Oficial da União*, 23 nov. 2007, Seção I, Brasília, p. 252, 2007. Disponível em: <http://www.portalmédico.org.br/resolucoes/CFM/2007/1821_2007.pdf>. Acesso em: 18 jun. 2019.

²⁶ FELITTI, Chico. Brecha em aplicativo do SUS expôs informações de saúde até de Temer. *In: Folha de S. Paulo*. 2018. Disponível em: <<https://www1.folha.uol.com.br/cotidiano/2018/01/1953472-brecha-em-aplicativo-do-sus-expos-informacoes-de-saude-ate-de-temer.shtml>>. Acesso em: 20 jun. 2019.



informação são alternativa promissora para a redução dos custos, ampliação do acesso e para a melhoria dos serviços de saúde, pois “[...] muitos dos gastos com saúde são ineficientes, derivados da escassez de informação e da repetição de exames desnecessários”²⁷.

Ainda, o cruzamento de dados pode detectar e prevenir o crescimento de doenças e possíveis invasores à saúde, como vírus e bactérias. A partir da navegação online dos cidadãos a respeito de sintomas físicos e as doenças a eles relacionadas, em sites de buscas, criam-se padrões de dados que contribuem para a detecção da localização de tais pessoas e para o posterior exercício de políticas públicas de contenção ou prevenção²⁸. Nesse contexto, Rafael Rocha e Marcos d’Ornellas esclarecem que:

Ao mesmo tempo em que os bancos de dados médicos são extremamente benéficos para a profissão médica, a sua própria natureza prejudica a confidencialidade dos dados. No sentido de promover a proteção dos direitos de confidencialidade do paciente, deve-se aumentar a segurança dos bancos de dados através de medidas técnicas e também legais. Embora isto possa causar um esforço adicional para os profissionais da área médica, é sempre necessário preservar a relação médico paciente²⁹.

Sobremaneira, os bancos de dados informatizados estruturam-se em acordo com uma lógica utilitarista, visando à formação de valor ao dado coletado, e à composição de um verdadeiro ativo imaterial. Tal afirmação resulta clara ao verificar-se a utilização maciça de bases de dados de saúde pela indústria farmacêutica, como forma de mapeamento de doenças e consequente utilização dos fármacos, prática que resulta na criação e indexação de perfis e indicadores regionais, além da utilização de perfis e históricos médicos para limitar a cobertura dos planos de saúde de alguns pacientes.

Constata-se, desse modo, a manifesta imprescindibilidade da proteção à privacidade e aos dados pessoais dos pacientes e dos usuários dos sistemas de saúde,

²⁷ NEGRI, Fernanda de. As tecnologias da informação podem revolucionar o cuidado com a saúde? **Radar: tecnologia, produção e comércio exterior**, v. 57, p. 31-33, 2018. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/radar/180827_radar_57.pdf>. Acesso em: 20 jun.2019.

²⁸ MAYER-SCHÖNBERGER, Viktor; CUKIER, Kennet. **Big Data: la revolución de los datos masivos**. Madrid: Turner Publicaciones, 2013.

²⁹ D’ORNELLAS, Marcos Cordeiro; ROCHA, Rafael Port da. Acesso e Privacidade: Em Busca da Segurança das Informações em Bancos de Dados Médicos. In: VII CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE, São Paulo, 2000. **Anais do VII Congresso Brasileiro de Informática em Saúde**. São Paulo, 2000, p. 76-81.



frente aos desafios que emergem do uso das novas tecnologias, no registro e no tratamento, em grande volume, das informações de caráter pessoal.

As recentes revoluções tecnológicas, que redundaram na criação de bancos ou bases de dados, e no tratamento desses de forma maciça, desafiam e banalizam a ótica da proteção dos dados médicos e pessoais tão somente pelo modelo individualista do consentimento informado e esclarecido. A doutrina moderna, em razão da dificuldade no controle do uso que será feito da informação pessoal, haja vista a amplitude no tratamento indiscriminado dessa, já sugere a criação de um modelo de proteção a partir de uma visão coletiva, que abranja o bem comum social e efetive a tutela dos dados de maneira ampla e condizente com a realidade prática.

Dessa forma, diante das inúmeras possibilidades de armazenamento e de difusão de informações na sociedade em rede, é de extrema importância que se compreenda e discuta acerca da tutela do direito de privacidade e da autodeterminação informativa do paciente, especialmente quanto às iniciativas de e-Saúde. Tal tema, ainda em construção, sofre o impacto da nova legislação específica brasileira sobre proteção de dados pessoais, de 2018, razão pela qual é necessária a observância aos direitos fundamentais do paciente quanto os dados de saúde.

CONCLUSÃO

A partir da confecção deste trabalho, têm-se algumas conclusões. Primeiramente, restou evidente que o Brasil iniciou corrida hercúlea para alcançar os países desenvolvidos no nível de proteção conferida aos dados pessoais, especialmente no nível legislativo. O primeiro passo foi a promulgação da Lei Geral de Proteção dos Dados Pessoais (LGPD), em 2018, que - espera-se - possibilitará ao cidadão ferramentas de controle e transparência quanto a real utilização de seus dados, frente ao direcionamento exponencial de aspectos pessoais, profissionais, empresarias e administrativos para os meios digitais.

A cidadania integral do brasileiro e do usuário de sistemas de saúde, na atual sociedade em rede e informacional, impôs a atualização e modernização do ordenamento jurídico do país, fato que oportuniza, desde já, a abertura de consciência quanto à dimensão e importância do tema, renovando-se o conceito tradicional de intimidade e privacidade. A novel regulamentação de proteção de dados balizará, quando plenamente



em vigor, posicionamentos jurisprudenciais condizentes à dinâmica hoje vivenciada, e fomentará a produção literária e doutrinária sobre o tema, refinando-se conceitos e teorias e estabelecendo-se regras cada vez mais claras e protetivas ao cidadão.

Na área da saúde, em específico, a tutela das informações de caráter pessoal dos pacientes foi concebida, inicialmente, por normas éticas e setoriais da classe médica, expostas em regulamentos e Códigos de Ética publicizados e adotados pelo Conselho Federal e pelos Conselhos Regionais de Medicina, os quais não abrangem os demais profissionais da saúde que igualmente possuem contato direto com os dados médicos das pessoas.

A chegada e a introdução das tecnologias de informação e comunicação (TIC), por meio dos serviços, facilidades e técnicas de e-Saúde, a exemplo das teleconsultorias, da educação permanente à distância, da formação de redes colaborativas, na adoção de prontuários digitais e bancos de dados de saúde informatizados, reverberou na estratégia das gestões empresariais, médicas e hospitalares, por ter modificado amplamente a coleta, o processamento e o armazenamento dos registros médicos dos pacientes.

Por fim, conclui-se que a atuação jurídica deve ser aliada das novas tecnologias, e não o contrário. A pesquisa no campo da informática em saúde manifesta-se como o principal vetor de mudança positivo deste cenário, ao incentivar, como forma de proteção, o uso de *softwares* e sistemas com o devido uso de senhas, certificado de segurança, criptografia de dados, segurança de rede, etc.

Nesse sentido, no âmbito jurídico, há que ocorrer a superação do conceito estático de privacidade, dissociado do contexto fático vivenciado pela sociedade e da necessidade de adoção da proteção dos dados pessoais como um direito fundamental humano, haja vista sua influência na formação da personalidade exteriorizada pelos indivíduos. A interpretação das normas constitucionais atinentes aos direitos de privacidade e intimidade deve ser fiel ao tempo presente, vivenciado pela sociedade em rede e informacional, reconhecendo-se a relação direta entre tais direitos e a comunicação e o tratamento dos dados pessoais, especialmente os sensíveis, como os de saúde.

A exemplo de outros países, a recente Lei Geral de Proteção dos Dados Pessoais no Brasil constitui-se como um importante marco normativo para a tutela de direitos fundamentais na Rede, inclusive com respeito à autodeterminação informativa. Todavia, devem ser adotadas estratégias no sentido de que o direito à privacidade do paciente seja



efetivamente protegido, mesmo diante das iniciativas de e-Saúde para a informatização dos dados dos pacientes.

REFERÊNCIAS

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. 1. ed. Traduzido por Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BORROZZINO, Nélio Fernandes; PIZA, Ivan Torres. Aspectos legais do Prontuário Eletrônico do Paciente: Um Comparativo do Cenário Atual Frente a Resolução do CFM. **Ciência et Praxis**, Belo Horizonte, v. 8, n.15, p. 23-27, 2015. Disponível em: <<http://revista.uemg.br/index.php/praxys/article/view/2150/1142>>. Acesso em: 18 jun. 2019.

BRANDEIS, Louis D.; WARREN, Samuel D. *The Right to Privacy*. **Harvard Law Review**, v. IV, 1980. Disponível em: <http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html>. Acesso em: 16 jun. 2019.

BRASIL. Governo Federal. **Aplicativo vai ampliar o acesso da população às informações de saúde**. 2017. Disponível em <<http://www.brasil.gov.br/saude/2017/06/aplicativo-vai-ampliar-o-acesso-da-populacao-as-informacoes-de-saude>>. Acesso em 30 jun. 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 14 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 jun. 2019.

CASTELLS, Manuel. **A sociedade em rede** - a era da informação: economia, sociedade e cultura. 5. ed. Traduzido por Klauss Brandini Gerhardt e Roneide Vanancio Majer. São Paulo: Paz e Terra, 1999.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.821/2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. **Diário Oficial da União**, 23 nov. 2007, Seção I, Brasília, p. 252, 2007. Disponível em: <http://www.portalmedico.org.br/resolucoes/CFM/2007/1821_2007.pdf>. Acesso em: 18 jun. 2019.

D'ORNELLAS, Marcos Cordeiro; ROCHA, Rafael Port da. Acesso e Privacidade: Em Busca da Segurança das Informações em Bancos de Dados Médicos. In: VII CONGRESSO BRASILEIRO DE INFORMÁTICA EM SAÚDE, São Paulo, 2000. **Anais do VII Congresso Brasileiro de Informática em Saúde**. São Paulo, 2000, p. 76-81.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, v. 12, p. 91-108, 2011. Disponível em: <<http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315/658>>. Acesso em: 30 jun. 2019.

ESTADOS UNIDOS DA AMÉRICA. **Records, computers and the rights of citizens**. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 07 de janeiro de 1973. Disponível em: <<https://aspe.hhs.gov/report/records-computers-and-rights-citizens>>. Acesso em: 21 jun. 2019.



FELITTI, Chico. Brecha em aplicativo do SUS expôs informações de saúde até de Temer. *In: Folha de S. Paulo*. 2018. Disponível em: <<https://www1.folha.uol.com.br/cotidiano/2018/01/1953472-brecha-em-aplicativo-do-sus-expos-informacoes-de-saude-ate-de-temer.shtml>>. Acesso em: 20 jun. 2019.

FRANÇA, Genival Veloso de. **Direito médico**. 14. ed. rev. e atual. Rio de Janeiro: Forense, 2017.

HOCH, Patrícia Adriani. **Levando a intimidade a sério no contexto da sociedade em rede**. Dissertação (Mestrado). Universidade Federal de Santa Maria, 2017.

KAMEDA, Koichi; PAZELLO, Magaly. E-Saúde e desafios à proteção da privacidade no Brasil. *PolITICs*, v. 16, p. 31-40, 2013. Disponível em: <<https://politics.org.br/edicoes/esa%C3%BAde-edesafios-%C3%A0-prote%C3%A7%C3%A3o-da-privacidade-no-brasil>>. Acesso em: 20 jun. 2019.

LIMBERGER, Temis. **O direito na era da informática: a necessidade de proteção dos dados pessoais**. Porto Alegre: Livraria do Advogado, 2007.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kennet. **Big Data: la revolución de los datos masivos**. Madrid: Turner Publicaciones, 2013.

NEGRI, Fernanda de. As tecnologias da informação podem revolucionar o cuidado com a saúde? **Radar: tecnologia, produção e comércio exterior**, v. 57, p. 31-33, 2018. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/radar/180827_radar_57.pdf>. Acesso em: 20 jun. 2019.

PARANHOS, Denise G.A.M.; ALBUQUERQUE, Aline. Direitos humanos dos pacientes como instrumentos bioéticos de proteção das pessoas idosas. **Cadernos Ibero-Americanos de Direito Sanitário**, Brasília, v. 8, n.1, p. 53-64, 2019. Disponível em: <<https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/issue/view/30/showToc>>. Acesso em: 18 jun. 2019.

PEREZ LUÑO, Antonio Enrique. **Derechos Humanos, Estado de Derecho y Constitución**. Madrid: Editorial Tecnos, 2005.

REZENDE, Edson José Carpintero; MELO, Maria do Carmo Barros de; TAVARES, Eduardo Carlos; SANTOS, Alaneir de Fátima dos; SOUZA, Cláudio de. Ética e Telessaúde: reflexões para uma prática segura. **Panam Salud Publica**, v. 28, p. 58-65, 2010. Disponível em: <https://scielosp.org/scielo.php?pid=S1020-49892010000700009&script=sci_abstract&tlng=pt>. Acesso em: 28 jun. 2019.

SIMÃO FILHO, Adalberto; SCHWARTZ, Germano André Doederlein. “Big Data” Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review**, v. 2, n. 3, p. 311-331, 2016. Disponível em: <<http://portaltutor.com/index.php/conpedireview/article/view/314/pdf>>. Acesso em: 21 jun. 2019.

UNIÃO EUROPÉIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Bruxelas, L 119, p. 1 - 88. Disponível em: <<https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT>>. Acesso em: 19 jun. 2019.