O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana

Gabrielle Bezerra Sales SARLET[*]

Cristina CALDEIRA[**]

RESUMO: O modelo informacional alterou a gramática cultural da Sociedade, encetando novos conflitos ainda isentos de adequada regulamentação jurídica e impelindo uma análise a partir do princípio da dignidade da pessoa humana, dos direitos humanos e fundamentais previstos nas constituições brasileira e portuguesa que, nessa medida, forjaram os alicerces éticos e jurídicos dessa investigação teórica encetada mediante o emprego do método bibliográfico e de uma abordagem exploratória e descritiva sobre a proteção dos dados de saúde, particularmante com o enfoque voltado para o atual contexto engendrado a partir da recente promulgação da Lei Geral de Proteção de Dados brasileira em evidente sintonia com a regulamentação européia em vigor a partir de maio, enfatizando, portanto, a relevância do consentimento livre e informado como o principal instrumento para assegurar, em uma perspectiva multinível, a integralidade dos direitos e das garantias à pessoa humana, dentro e fora do ambiente digital.

PALAVRAS-CHAVE: Dados pessoais; consentimento informado; saúde; internet; era da informação.

TITLE: The Informed Consent and the Protection of Personal Health Data on the Internet: An Analysis of the Legislative Experiences of Portugal and Brazil for the Integral Protection of the Human Person

ABSTRACT: The informational model changed the cultural grammar of the Society, starting new conflicts still exempt from adequate legal regulation and impelling an analysis based on the principle of human dignity and the human and fundamental rights foreseen in the Brazilian and Portuguese constitutions that, to this extent, lay the foundations ethical and legal aspects of this theoretical investigation initiated through the use of the bibliographic method and an exploratory and descriptive approach on the protection of health data, particularly with the focus on the current context generated since the recent enactment of the General Law on Data Protection Brazilian legislation in effect

[*] Advogada, graduada e mestre em Direito pela Universidade Federal do Ceará, doutora em Direito pela Universidade de Augsburg – Alemanha, Pós- doutora em Direito pela Universidade de Hamburg – Alemanha, pós-doutoranda em Direito pela PUCRS e, atualmente, professora dos cursos de graduação, de pós-graduação e do mestrado em Direito no Centro Universitário Ritter dos Reis- Uniritter. Ex-bolsista do Max-Plank-Institut für ausländisches und internationales Privatrecht Hamburg.

[**] Jurista, Professora Auxiliar, desempenhou funções de Adjunta da Secretária de Estado do Ministério da Ciência, Tecnologia e Ensino Superior. Coautora de projetos de diplomas legais. Investigadora de Pós-Doutoramento na área da Propriedade Intelectual, Universidade Nova de Lisboa. Colabora no Laboratório de Bioética no Hospital de Clínicas (RS Brasil), como investigadora na área de proteção de dados biomédicos. Programa Doutoral em Ciência Política na especialidade de políticas públicas, Universidade Católica Portuguesa. Doutorada em Direito na Especialidade em Ciências Jurídicas e Políticas pela Universidade Autónoma de Lisboa (UAL) e Bolseira da Fundação Gulbenkian na Universidade de Oxford, St Antony's College.

in May, emphasizing, therefore, the relevance of free and informed consent as the main instrument to ensure, in a multilevel perspective, the integrality of rights and guarantees to the and outside the am digital environment.

KEYWORDS: Personal data; informed consent; health; internet; information age.

1. Notas introdutórias

Dados pessoais são todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular, enquanto os dados sensíveis são aqueles que tratam sobre a origem racial e étnica, as convicções políticas, ideológicas, religiosas, as preferências sexuais, os dados sobre a saúde, os dados genéticos e os biométricos. O conjunto dessas informações compõe os perfis ou as identidades digitais, possuindo valor político e, sobretudo, econômico, vez que podem ser a matéria prima para o uso de *softwares* diretamente atrelados às novas formas de controle social, especialmente mediante o uso de algoritmos. Daí, a proteção de dados é, em síntese, a proteção da pessoa humana, mormente o resguardo do livre desenvolvimento de sua personalidade e, em particular, por meio da garantia da sua autodeterminação informacional.

Em verdade, uma consequência imediata do advento da Internet foi a ilusão de que se tratava de ambiente absolutamente neutro e, consequentemente, seguro. Tal situação acarretou, dentre outras coisas, uma espécie de deslocamento de um considerável contingente populacional situado às margens do conhecimento formal, a dizer, afetados pela divisão digital, que, fascinado, cede sem maior zelo os seus dados pessoais, inclusive os dados sensíveis, notadamente os dados de saúde, para alcançar uma possibilidade de acesso a um simulacro de cidadania digital e, desse modo, se sentir incluído. Adensando, pois, o desnivelamento cultural e digital entre os países.

No entanto, convém enfatizar que a popularização[1] da tecnologia da informação, por sua vez, gerou frutos revolucionários que perpassam desde a quantidade de dados que são

[1] Na primeira década do século XXI, o número de pessoas conectadas à Internet passou de 350 milhões para 2 bilhões. Além disso, neste mesmo período, o número de pessoas com celulares passou de 750 milhões para 5 bilhões. A expectativa para o ano de 2025 é de que a maior parte da população mundial estar com acesso à informação instantânea, sendo que, se for mantido o ritmo de crescimento de pessoas conectadas à Internet, ter-se-á, na mencionada data, 8 bilhões de pessoas *online*. SCHMIDT, Eric – COHEN, Jared. *The New Digital Age: Reshaping the Future of People, Nations and Business*. London: John Murray, 2014, p. 15.

atualmente disponibilizados, o custo energético[2], os locais apropriados para o armazenamento e a segurança, a virtualidade[3] das relações sociais e até a velocidade com que esses dados trafegam na rede e atingem a locais antes impensáveis para o ser humano, além da outrora aludida ilusão de neutralidade que envolve a todos nesse processo de virtualização do cotidiano[4].

Além disso, oportunizou o uso da biotecnologia de forma extremamente singular e, nessa medida, alcançou novos patamares para tratamentos na área da saúde, forjando uma era genômica, incluindo a revolucionária inserção da TIC- tecnologia de informação e de comunicação na relação do paciente com os profissionais de saúde e, assim, encetando um novo panorama sócio-cultural em função da possibilidade de comunicação ubíqua das máquinas e dos equipamentos derivada do acentuado uso da inteligência artificial no campo da medicina.

Interessante sublinhar as novas fissuras nessa relação sob o ponto de vista da garantia real da confidencialidade em ambiente digital, inclusive gerando reflexos sobre a produção da diagnose e, por derivação, na redefinição de padrões éticos na área da saúde. Com efeito, algumas consequências já são percetíveis, enquanto outras ainda apontam para um prognóstico de uma abissal clivagem na História da Humanidade[5]. Incontestavelmente, a

[2] AFINAL, quanta energia elétrica a internet utiliza para funcionar? *TECMUNDO*. Disponível em: <https://www.tecmundo.com.br/internet/104589-quanta-energia-eletrica-internet-utiliza-funcionar.htm> Acesso em: 17 jan. 2018. Em 2011 a internet dos EUA consumiu em media 2% de toda a energia elétrica produzido no mundo. O calor gerado pelos servidores, ativos ou não, exige resfriamento compatível e, dessa forma, estima-se que em 2020, nos EUA, o consumo deva subir para 140 bilhões de kWh, 54% a mais.

[3] AGAMBEN, Giorgio. *Lo abierto: el hombre y el animal*. Flavia Costa y Edgardo Castro (Trad). Buenos Aires: Adriana Hidalgo, 2006, p. 35.

[4] Por neutralidade se entende o princípio que garante que todo conteúdo transmitido pela rede de computadores deve ser tratado da mesma maneira, isto é, sem sofrer qualquer espécie de discriminação, seja por seu conteúdo, por sua origem ou por seu destino. Por todos, conferir, MARSDEN, C.T. *Net Neutrality: towards a Co-Regulatory Solutions*. Londres: Bloomsburry Academic, 2010, p. 36.

[5] RAMSAY, Iain. *Consumer protection in the era of informational capitalism*. In: WILHELMSSON, Thomas; TUOMINEM, Salla; e TUOMOCA, Heli (ed.) Consumer law in the information society. The Hague. Kluwer Law International, 2001, p. 45.

revolução do uso da tecnologia da informação provocou profundas alterações nas relações sociais, gerando efeitos políticos, econômicos[6], patrimoniais, jurídicos[7] e existenciais[8].

De acordo com a recente fonte normativa europeia, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, doravante RGPD, a União Europeia introduziu alterações importantes sobre a proteção das pessoas singulares relativamente ao tratamento de dados pessoais, com especial impacto sobre os dados de saúde, consequentemente sobre os dados sensíveis que, independentemente do formato com que são coletados, vêm impôr novas obrigações aos cidadãos e a todas as instituições, públicas e privadas, ao exigir a adoção de medidas técnicas e organizativas adequadas[9].

A especificidade da informação de saúde implica a análise lúcida e crítica desse contexto no qual o tratamento da informação se desenrola, sobretudo em razão da sua finalidade particular. "O contexto é a relação terapêutica que é estabelecida entre a pessoa e o profissional de saúde, ao passo que a finalidade da sua revelação - a assistência (traduz-se na) intervenção diagnóstica, terapêutica ou paliativa."[10]. Tratando-se de dados sensíveis, reafirma-se a exigência de uma proteção especial alicerçada no princípio da dignidade da pessoa humana, o "sismógrafo que indica o que é constitutivo de uma ordem jurídica democrática"[11]. Este reforço antropológico encontra ainda amparo no artigo 2.º do Tratado da União Europeia (TUE), no qual se consagra, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos humanos.

---

[6] Para uma percepção da monetarização do uso da internet, oportuno lembrar que a Microsoft adquiriu em 2016 a Linkedin, pagando 26 milhões de dólares pela empresa e, principalmente, pelo seu cadastro profissional de 430 milhões de usuários e 100 milhões de visitantes por mês. O valor representa 60 dólares por usuário ou 260 dólares por visitante mensal. *In:* The Economist. LinkedUp. Disponível em: <http://www.economist.com/news/business_and_finance/21700605_it_one_most_expensive_tech_deals_history_it-may_not_be_smartest_making_sense>. Acesso em: 03 jan. 2018

[7] LEITE, Flávia Piva Almeida. *O Exercício da Liberdade de Expressão nas Redes Sociais e o Marco Civil da Internet*. In Revista de Direito Brasileiro, vol. 13, n. 06, 2016, p. 150: "Sociedade da Informação – que nada mais é do que uma forma específica de organização social em que a gestão, o processamento e a transmissão de informações tornam-se as fontes fundamentais de produção e de poder, devido às novas condições tecnológicas surgidas nesse período histórico. O surgimento dessa nova sociedade trouxe, portanto, a necessidade de repensar o papel do Estado nesse novo contexto.

[9] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, considerando 78.

[10] DEODATO, Sérgio. *A proteção dos dados pessoais de saúde*. Porto: Universidade Católica Portuguesa, 2017, p. 16.

[11] HABBERMAS, Jürgen. *Um Ensaio sobre a Constituição da Europa*. Trad. Mrian Toldy; Teresa Toldy. Lisboa: Edições 70 Lda, 2012. Título original: *Essay zur Verfassung Europus* (2011), p.37.

Com efeito, observando atentamente a contemporaneidade, verifica-se que há um alinhamento dos países, com destaque entre os Estados-membros da União, em relação ao modo de enfrentamento do problema da proteção de dados, em especial no que afeta à segurança e à transmissibilidade, vez que sua complexidade[12] se tornou evidente na medida em que manifesta *prima facie* uma dimensão existencial a despeito da inconteste amplitude patrimonial.

Imbuído destes referenciais, o legislador português consagrou, em termos genéricos, o regime jurídico português de proteção de dados pessoais na Lei de Proteção de Dados Pessoais, Lei nº 67/98, de 26 de outubro, a qual abrange a categoria dos dados pessoais relativos à saúde na internet. Este diploma será brevemente revogado pela nova Lei de Proteção de Dados. O artigo 2.º da Lei nº 67/98, de 26 de outubro, enuncia o princípio geral da transparência e da defesa da privacidade. A mesma consagração, diga-se de passagem, está plasmada em várias normas de diplomas específicos do direito da saúde.

Em síntese, não se pode olvidar que estão em causa dados pessoais, que são considerados ativos financeiros e que em uma composição contemporânea logram uma nova corrida pelo ouro nos Estados menos desenvolvidos para fins de novas modalidades de dominação, particularmente em áreas sensíveis como a que envolve o complexo fenômeno da saúde que, sinteticamente, se expande muito além da lógica do adoecimento e da cura. Daí, evidencia-se a pertinência de estudos que, se orientam para a desmistificação da neutralidade do emprego da biotecnologia, de modo geral e, em particular visam o descortinamento dos possíveis agravos à pessoa humana, nesse novo panorama para, diante das novas circunstancias, compor pautas de soluções apropriadas ao contexto transfronteiriço que tangencia o tema.

Nesse intento, essa investigação teórica, bibliográfica e eminentemente exploratória, parte da análise das premissas estabelecidas acerca dos principais eixos contemporâneos do Estado democrático de Direito, destacando-se a privacidade e a proteção de dados na era da informação, estabelecendo o consentimento livre e informado como um relevante instrumento para a garantia da proteção dos dados na área da saúde, notadamente tendo como base as contribuições advindas do sistema normativo europeu e, em particular, do

[12] STATZEL, Sophie. *Cybersupremacy: The new Face and Form of white Supremacy Activism*. In: Digital Media and Democracy: Tactics in hard Times. Megan Boler (Edit.). Cambridge: MIT Press, 2008, p. 409.

português para a proposição de pautas de solução apropriadas à multiplicidade de conflitos advindos do emprego da tecnologia no panorama brasileiro recentemente alterado com a promulgação de uma Lei geral de proteção de dados pessoais e, portanto, carecendo ainda de reflexão e de amadurecimento que resguardem a sua concreta efetividade.

2. Privacidade e proteção de dados da saúde na era da informação face às múltiplas possibilidades de danos no contexto de *Big Data*

A tentativa de regulamentação da proteção de dados remonta aos anos 70 do século XX, ocasião em que o Estado era o maior responsável pelos dados armazenados e, nesse sentido, torna-se oportuno lembrar que a Alemanha foi pioneira na tarefa de vislumbrar os riscos e apontar itinerários de garantias. Atualmente, as entidades privadas, notadamente no que afeta à saúde e em especial em relação às seguradoras, aos conglomerados de hospitais e à indústria farmacêutica, são o alvo principal das modalidades de regulamentação para a concretização da plena democracia digital[13], cujo núcleo essencial é o protagonismo da pessoa humana, especialmente por meio do reconhecimento da preponderância do consentimento informado de seus partícipes.

De qualquer modo, interessa reafirmar que no século XXI, o sistema capitalista passou por uma reestruturação em seu modo de produção e, assim, houve a criação de uma nova estrutura social, a qual foi denominada por Castells como *informacionalismo*. Segundo Castells, "no informacionalismo, as tecnologias assumem um papel de destaque em todos os segmentos sociais, permitindo o entendimento da nova estrutura social – sociedade em rede – e consequentemente, de uma nova economia, na qual a tecnologia da informação é considerada uma ferramenta indispensável na manipulação da informação e construção do conhecimento pelos indivíduos", pois "a geração, processamento e transmissão de informação torna-se a principal fonte de produtividade e poder"[14]. De sorte que a informação passou a ser a matéria prima mais valiosa. No mesmo sentido, Pierre LÉVY observa que,

> O ciberespaço (que também chamarei de 'rede') é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.[15]

[13] SUNSTEIN, Cass R. *Republic: divided democracy in the age of social media*. New Jersey: Princeton University Press, 2017, p. 138.
[14] CASTELLS, Manuel. (1999). *A Era da Informação: economia, sociedade e cultura*. Vol. 3. São Paulo: Paz e terra, p. 21.
[15] LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2008, p 17.

Em escala global, muitos sustentam que os dados e a informação ocupam um lugar de destaque e de importância para a sociedade, sendo considerados o verdadeiro petróleo da era digital, conforme destacado em reportagem publicada em 06 de maio de 2017 pela revista The Economist, "*A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era*.[16]" Em face desse contexto, e.g., pode-se afirmar que o direito à proteção de dados pessoais no ordenamento jurídico brasileiro é considerado um direito fundamental implícito, que como denota Ingo Sarlet, engloba: o direito de acesso e conhecimento dos dados pessoais existentes em registros (banco de dados) públicos e privados; o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; o direito ao conhecimento da finalidade da coleta e eventual utilização dos dados; o direito à retificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados.[17]

Tal reconhecimento coaduna com o RGPD, instrumento jurídico de direito secundário europeu, que entrou plenamente em vigor no dia 25 de maio de 2018, com o objetivo de uniformizar o regime de tratamento de dados no espaço da União Europeia, requisito essencial para o bom funcionamento do Mercado Único. Este novo instrumento jurídico, assenta em uma maior responsabilidade, informação e transparência e, ainda que não constitua uma completa ruptura com a legislação anterior, as consequências da sua aplicação geram alterações paradigmáticas na forma como é realizado o tratamento de dados pessoais, ou seja, coloca a pessoa e a defesa dos seus direitos constitucionalmente consagrados, no centro do debate.

Na Europa, cresceu o entendimento de que o RGPD, instrumento que revogou a Diretiva 95/46/CE, de 24 de outubro de 1995, é a base jurídica específica de raiz antropológica que faltava à União Europeia, para proteger integralmente a pessoa. A despeito de compartilhar com esta visão, entende-se que, de fato, ela é fruto de um somatório, resultando de um

[16] THE Economist. *The world's most valuable resource is no longer oil, but data*. Disponível em <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> . Acesso em: 01jun.2018.
[17] MARINONI, Luis Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. *Curso de Direito Constitucional*. São Paulo: Revista dos Tribunais, 2014, p. 434-435.

conjunto de instrumentos jurídicos relevantes que foram sendo criados ao longo do século XX, dos quais se destacam: *Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais*, (1950), consagra no artigo 8.º o direito ao respeito pela vida privada e familiar: «Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pela sua correspondência;*Convenção 108 para a Proteção das Pessoas Singulares* (1981), do Conselho da Europa, debruçou-se sobre o Tratamento Automatizado de Dados Pessoais.

De fato, trata-se do primeiro instrumento internacional juridicamente vinculativo adotado no domínio da proteção de dados. O objetivo era «garantir [...] a todas as pessoas singulares [...] o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de caráter pessoal. O Tratado de Lisboa (2009), dessa maneira, apresenta-se como uma nova fase da União Europeia, na qual se reforça a proteção de dados pessoais, quer por meio da influência do Tratado sobre o Funcionamento da União Europeia (TFUE), quer mediante a Carta dos Direitos Fundamentais da União Europeia (CDFUE)[18].

De todo modo, estes dois instrumentos são determinantes para a evolução dos Estados-Membros nesta matéria, a saber: no artigo 16.º do TFUE, é introduzida uma base jurídica específica para a adoção de regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições da União e pelos Estados-Membros, o n. 1 do artigo 8.º da CDFUE, defende que "Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito."

Nessa conformidade, os dados pessoais "devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação" (n.º 2). A CDFUE, foi formalmente adotada em Nice (2000), consagra a defesa dos direitos e das liberdades fundamentais das pessoas singulares e reconhece o respeito pela vida privada e familiar no artigo 7.º. No artigo 8.º protege os dados pessoais como direitos fundamentais estritamente relacionados, mas

[18] CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2000/C 364/1), publicada no Jornal Oficial das Comunidades Europeias (JOCE), de 18-12-2000. Disponível em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf.

distintos. Atualmente, a CDFUE está integrada no Tratado de Lisboa (2009) e é juridicamente vinculativa nas instituições e nos órgãos da União e nos Estados-Membros, quando aplicam legislação da União Europeia.

Portanto, com a criação da *Estratégia para o Mercado Único Digital*[19], em 2015, a Europa continuou empenhada em aproveitar "as oportunidades oferecidas pelas tecnologias digitais, que não conhecem fronteiras e quebrar as barreiras nacionais em matéria de regulamentação das telecomunicações, de direitos de autor e de proteção dos dados"[20]. Nessa conformidade, enfatiza-se ainda que essa temática deve ser analisada à luz da proposta de Regulamento sobre Privacidade e Comunicações Eletrónicas (Regulamento e-Privacy)[21], isto é, na medida em que se trata de um novo instrumento jurídico integrado na supracitada *Estratégia para o Mercado Único Digital*.

De fato, a evolução tecnológica permitiu a criação de aparelhos e de procedimentos médicos automatizados e "ironicamente, a procura inicial por serviços médicos robotizados pode vir da parte das economias emergentes e não dos mercados instuídos, como os Estados Unidos ou a Europa"[22]. A saúde é um exemplo peculiar dessa crescente automatização e da aplicação da robótica em ambiente laboratorial e farmacêutico, inclusive em razão de sua posição nuclear na vida humana e da condição de vulnerabilidade com que a pessoa normalmente se insere nesse âmbito, incrementando exponencialmente o volume das pegadas[23] digitais. Por toda a Europa, porém, crescem a oferta e a demanda por serviços digitais aplicados à saúde e, sobretudo, em contextura de Big Data (os megadados) que resultam da coleta, do armazenamento e do tratamento automatizado de um conjunto enorme e variado de dados.

Assim, prenhe de expectativa Portugal aderiu ao *eHaelth Summit* e, em 2018, pelo segundo ano consecutivo, organizou o *Portugal eHealth Summit*, durante o qual, foram discutidos os desafios e as oportunidades do processo de transformação digital de saúde. Em se tratando

---

[19] COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES Estratégia para o Mercado Único Digital na Europa. COM/2015/0192 final.

[20] COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES Estratégia para o Mercado Único Digital na Europa. COM/2015/0192 final.

[21] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE. COM/2017/010 final - 2017/03 (COD).

[22] PUGLIANO, John. *Os robôs querem o seu emprego*. Portugal: Porto Salvo, 2018, p. 157.

[23] BRUNO, Fernanda. *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina, 2013, p. 123.

de um sistema demasiadamente complexo que envolve diversos órgãos e pessoas, a e-Saúde oferece alguns riscos à confidencialidade inerente à relação médico-paciente e à segurança do tratamento e da livre circulação dos dados de saúde. Ou seja, trata-se de todas as informações sobre o estado físico ou mental dos cidadãos, incluindo as que se referem à prestação de serviços que revelem informações sobre as suas condições de saúde. A perda da confidencialidade pode occorer à medida que são utilizadas aplicações em dispositivos inteligentes, por meio das quais vão sendo recolhidas cada vez maiores quantidades de dados para o tratamento e para prestações de serviços inovadores, podendo, entretanto, ser sujeitas a diversas modalidades de tratamento posterior, tendo em vista fins economicos a despeito do consentimento do paciente.

Com base nessa realidade, José de Oliveira Ascenção alerta para o fato da informática permitir intromissões na vida privada, referindo que "as suas potencialidades são tais que a intimidade de todos está sujeita a ser devassada a todo o momento", pois "o cruzamento das informações respeitantes a cada pessoa desvela o retrato de toda a sua vida"[24]. Não obstante, assiste-se assim, por todo o mundo, a um processo de transformação digital da saúde a que designamos e-Saúde ou Cibermedicina e que conta já com bons exemplos em vários países: Alemanha (Eletronic Health Card), Brasil (verifica-se um aumento de aplicativos para celulares tendo em vista a saúde), Portugal (aplicativo Knok), Reino Unido (aplicativo Babylon), Suécia (website KRY) entre outros.

Last but not least, são enormes os desafios que os Big Data em uma correlação com a saúde impõem, vez que podem por em causa a segurança dos dados dos pacientes, a perda dos próprios dados que se encontram ao dispor das entidades de saúde bem como materializam de modo cada vez mais factível a possibilidade de ciber-ataques à informação de saúde.

[24] ASCENSÃO, José de Oliveira. *Estudos sobre direito da internet e da sociedade da informação*. Coimbra: Almedina, 2001, p. 264. Discorrendo sobre a proteção da intimidade no mundo da informática, diz Têmis Limberger que "o conteúdo da intimidade apresenta dois aspectos. O aspecto negativo é o vetusto direito a não ser molestado, que hoje protege o cidadão de intromissões externas de outros indivíduos ou do poder público" [...]. As novas tecnologias (entre elas a informática) encontram um limite na intimidade e em outros direitos fundamentais. Já o aspecto positivo da intimidade é o direito a exigir prestações concretas, tais como a informação, o acesso, a retificação e o cancelamento dos dados". (LIMBERGER, Têmis. *O direito à intimidade na era da informática:* a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007, p. 231).

Inconteste é a presença de riscos significativos, mormente para a garantia da confidencialidade e da privacidade[25] dos utentes dos serviços de saúde, e, nessa situação, em face de uma possível perda ou limitação injustificável de direitos e de liberdades fundamentais dos cidadãos. Estes desafios ganham maior dimensão tendo como critério a inescusável circulação de dados pessoais, com origem e destino em países em desenvolvimento. Estes movimentos transfronteiriços colocam obstáculos à interoperabilidade da informação de saúde, na medida em que se utilizam de formatos incompatíveis, para além das diferentes terminologias utilizadas pelos profissionais de saúde, a saber: CID, openEHR, etc.

Não custa reafirmar que as mudanças que são salientadas neste estudo, destarte, apresentam-se como desafios que ultrapassam todas as fronteiras territoriais e políticas, embora deva-se salientar que o principal enfoque será a partir da utilização do atual contexto europeu no que diz com a proteção de dados de saúde e, sobretudo, português, como um paradigma válido para a demanda de estruturação das medidas de segurança digital no Brasil. Nesta nova dimensão, torna-se imperioso enquadrar juridicamente a proteção de dados pessoais como um *direito fundamental global*, em outras palavras, direito humano, cujo âmbito de proteção se espraia em diversas frentes.

Torna-se inevitável o enfrentamento dos problemas jurídicos relacionados com a interoperabilidade entre sistemas, com a qualidade dos dados e da segurança dos mesmos, especialmente em matéria de informação de saúde, na medida em que se exige uma infraestrutura robusta e um amplo acesso à internet. Para ultrapassar estes desafios, a Comissão Europeia apresentou a *Proposta de Regulamento e-privacy*, em janeiro de 2017, um novo instrumento jurídico que estabelece um âmbito de aplicação material alargado, na forma em que abrange os tradicionais serviços de comunicações telefônicas (mensagem escrita ou correio eletrônico), mas igualmente outras comunicações que ocorrem via internet, designadamente os serviços over-the-top, como sejam o VOIP, serviços de messaging e webmail (e.g. Skype, WhatsApp e Gmail).

De toda sorte, a Proposta de Regulamento e-privacy, que vem reforçar a política de proteção dos dados iniciada pelo RGPD, também apresenta um alargamento do seu âmbito de

[25] CANCELIER, Mikhail Vieira de Lorenzi. *O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequencia (Florianópolis). N. 76. Ago2017. 213-240. p. 216. In: http://dx.doi.org/105007/2177-7055.2017v38n76p213 Acesso em: 16 ago. 2018.

aplicação territorial, passando a abranger toda a prestação de serviços de comunicações eletrônicas a utilizadores finais na União Europeia, independentemente da localização física do prestador ou do carácter oneroso da prestação. E caso o fornecedor de serviços de comunicações eletrónicas não tenha estabelecimento na União Europeia, deverá indicar, por escrito, um representante com poderes para interagir, em seu nome, com as autoridades de controle e os utilizadores finais sobre as matérias abrangidas pelo futuro Regulamento que se prevê para 2019. Assim, ao definir novos direitos e obrigações, tanto o RGPD como a Proposta de Regulamento e-privacy implicam em mudanças de procedimentos, de critérios, de atitudes com impacto nas comunicações eletrônicas transfronteiriças e, dessa maneira, intentam sinteticamente, firmar pilares de proteção em conformidade com o aumento das possibilidades de agravos e de danos à pessoa humana.

3. O consentimento informado como o principal instrumento de garantia dos dados pessoais relativos à saúde

Historicamente a obrigatoriedade do consentimento informado remonta às graves atrocidades vicenciadas durante a II Guerra Mundial. A banal utilização de prisioneiros nos campos de concentração em experiências médicas, dentre outros agravos, gerou uma nervura na História e conduziu à formulação do Código de Nuremberg (1947), que se constitui até hoje como o documento mais relevante da ética da investigação em seres humanos. Estas circunstâncias motivaram ainda a celebração de convenções, designadamente a Declaração Universal dos Direitos Humanos (1948), a Convenção Europeia dos Direitos Humanos (1950) e a Convenção de Helsinque (1964), revista no Brasil, mais especificamente na cidade de Fortaleza em 2013, constituindo-se em verdadeiros alicerces éticos e jurídicos para a proteção da informação de saúde na internet, notadamente por reconhecerem a dignidade, a liberdade e a autonomia do ser humano.

Igualmente digno de nota foi a elaboração do Relatório Belmont (1978) e do *Guia de Boas Práticas Clínicas* adotado pela OMS em 1995, que têm contribuído para a defesa da privacidade dos pacientes e dos participantes em ensaios clínicos, relacionando-a diretamente com o fortalecimento do consentimento informado como uma relação gnoseológica.

Com efeito, as relações na área da saúde devem ser configuradas a partir da construção de um ambiente de confiança, de horizontalidade e, em princípio, de liberdade. Na medida em

que se trata de área essencial da vida humana, a saúde passou a ser evidentemente muito afetada pelo emprego por vezes desordenado das inovações biotecnológicas, pela estruração de um mercado extremamente rentável e selvagem, pela aplicação irresponsável da tecnologia da informação e da comunicação e pelos novos paradigmas voltados para a imortalização e para o enaltecimento da ideia de perfeição em um contexto de saúde preventiva. Assim, em outro sentido, tangencia riscos de repaginação dos parâmetros eugênicos, gerando uma atmosfera de ideologização que se caracteriza, dentre outros aspectos, pelo fato de que, a despeito da proteção jurídica existente, devem ser franqueados todos os limites em função da promessa de uma vida em *high performance*.

Destaca-se, nessa altura, a fundamentalidade do ato de consentir, sobretudo no âmbito da internet, como fruto de uma relação gnoseológica, ou seja, como um processo de conhecimento em que, no caso, devem ser previamente esclarecidos em linguagem clara, precisa, apropriada e suficiente, a pertinência, a finalidade, a adequação, o tempo da coleta, o armazenamento, o tratamento e a transmissão dos dados obtidos no sentido de possibilitar a renúncia, a alteração, o uso, a cessão, e a disponibilidade ou a recusa daquele que consente. Afirma-se dessa maneira o papel do sujeito na condução e na construção de sua própria vida. Importando, nesses termos, garantir ainda a proteção contra os riscos de danos materiais e imateriais, e.g., em casos de criação de perfis falsos, violação da privacidade, retenção e manipulação de dados, estigmatização, discriminação[26], direta ou indireta por meio de cadastros etc.

Em alusão aos riscos na contemporaneidade e tendo em vista a urgência em definir a complexidade do ambiente digital, Santaella esclarece que:

> Em uma definição breve, o ciberespaço é o espaço informacional das conexões de computadores ao redor do globo, portanto um espaço que representa o conceito de rede e no qual a geografia física não importa, pois qualquer lugar do mundo fica à distância de um clique. [...] Hoje a troca de e-mails ficou muito rápida, o percurso para o acesso, cada vez mais simplificado, bastando o clique em uns poucos sinalizadores gráficos para alcançar o estatuto de uma conversação on-line que culmina no internet *relay chat ou no instant messaging*. Isso tudo sem que as mensagens tenham necessariamente que perder a consistência do texto escrito. Este pode ser copiado por scanners, e arquivos de textos, imagens, desenhos, sons e mesmos filmes podem ser anexados, o que faz do e-mail uma mídia de comunicação poderosa e, sobretudo, mista: tem a consistência sólida da escrita, mas, ao mesmo tempo, a fluidez dos líquidos.[27]

[26] ALMEIDA, Silvio Luiz de. *O que é racismo estrutural?* Belo Horizonte: Letramento, 2018, p. 56.
[27] SANTAELLA, Lucia. *Linguagens líquidas na era da mobilidade.* São Paulo: Paulus, 2011, p. 178.

Inegavelmente exsurge daí a ideia de reforçar a importância do consentimento, resgatando-o como um dos pontos de partida da abordagem bioética, pautada nos direitos humanos, e particularizando a sua natureza processual em que devem ser garantidas todas as condições, inclusive temporais e informacionais, para a tomada de decisão livre, esclarecida e autônoma em um cenário de responsabilidade[28].

O consentimento livre e informado é, em síntese, uma das principais garantias que norteiam a relação do paciente com os profissionais da saúde. Por outro lado, não se pode olvidar que a construção do processo de consentir implica, à guisa de exemplificação, o emprego de linguagem não diretiva e, no momento atual em que se sobressai o ambiente digital, aponta especialmente para a garantia da transparência no que tange à coleta, à finalidade, ao armazenamento, ao tratamento e à transmissão dos dados.

Oportuno enfatizar que a atual relação entre a proteção de dados pessoais e o processo de elaboração de consentimento na área da saúde corresponde na observância de um dever de garantir ao paciente a deliberação livre e, consequentemente, a revisão e a possibilidade de retirada da anuência a qualquer momento sem prejuízo algum, mediante a garantia de que o trafego desses dados não implicará em danos de espécie alguma. Em outras palavras, o consentimento deve ser efetuado nos moldes de um ato jurídico pleno, respeitando-se a ampliação de uma perspectiva de validade e de perfectibilidade em um panorama em que novos atores, advindos da era informacional[29], passam a ser cada vez mais co-responsáveis.

3.1. Uma mirada mais específica a partir do sistema normativo português

A problemática do consentimento informado e da proteção dos dados pessoais relativos à saúde na internet, vez em que se tratam de direitos que visam a proteção da pessoa humana, insta centrar a discussão a partir do artigo 35.º da Constituição da República Portuguesa (CRP) de 1976, no qual se consagra a proteção dos cidadãos perante o tratamento de dados pessoais informatizados (n. º 1), bem como, os dados pessoais constantes de ficheiros manuais (n. º 7). Verifica-se neste preceito, o alargamento do seu ambito de proteção, na medida em que regula a proteção de qualquer dado pessoal.

---

[28] BRÜGGEMEIER, Gert. *Protection of personality rights in the Law of delict/torts in Europe: mapping out paradigms*. In: BRÜGGEMEIER, Gert; CIACCHI, Aurelia Colombia; O'CALLAGHAN, Patrick. (Ed.). *Personality rights in european tort law*. Cambridge: Cambridge University Press, 2010.
[29] CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. *Big Data: A Revolution that will transform how we live, work and think*. Boston, New York: Mariner Books, 2014, p. 176.

Com efeito, o regime jurídico português de proteção de dados pessoais encontra-se consagrado, em termos genéricos, na Lei n. º 67/98, de 26 de outubro, Lei de Proteção de Dados Pessoais, que resultou da transposição da Diretiva n. º 95/46/CE e que será revogada por força da aplicação do RGPD. Não se pode olvidar, contudo, da existência de legislação específica para determinadas áreas, como é o caso da lei que regula o tratamento de dados pessoais no contexto das redes e dos serviços de comunicações eletronicas acessíveis ao público, Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto.

Tomando como referência o regime jurídico da informação de saúde em Portugal, podemos observar que a reflexão ética neste domínio e o quadro jurídico criado, nomeadamente a Lei da Informação Genética Pessoal e Informação de Saúde, Lei n. º 12/2005, de 26 de janeiro, alterada pela Lei n. º 26/2016, de 22 de Agosto, promove uma mudança paradigmática relativamente à titularidade dos dados pessoais de saúde. No seu artigo 3.º, o legislador adota o conceito de "informação de saúde", em detrimento dos dados de saúde, e consagra essa informação como sendo "propriedade" da pessoa a quem os dados dizem respeito. Neste conceito cabem todas as informações relativas à saúde de uma pessoa, especificamente os dados registrados nos processos clínicos, os resultados de análises e de outros exames subsidiários, das intervenções e dos diagnósticos, que são manejadas pelos profissionais de saúde na sua relação assistencial.

De forma inequívoca, o n. 1 deste artigo estabelece que "A informação de saúde, incluindo os dados clínicos registrados, resultados de análises e outros exames subsidiários, intervenções e diagnósticos, é propriedade da pessoa (...)". O legislador clarifica a titularidade dos dados de saúde, atribuindo às unidades do sistema de saúde a função de depositários da informação, a qual não pode ser utilizada para outros fins que não os da prestação de cuidados e da investigação em saúde e outros estabelecidos pela lei. Por esta razão, é indefensável que os dados de saúde dos pacientes registrados em instituições de saúde pública, sejam considerados "documentos administrativos". A natureza e a titularidade da informação não se alteram em função dos depositários da informação de saúde, sejam entidades públicas ou privadas.

Igualmente importante para esse estudo, é o teor da Lei 15/2014, de 21 de março, na versão do Decreto-Lei 44/2017, de 20/04, que veio consolidar a legislação em matéria de direitos e de deveres do utente dos serviços de saúde. Reforça o dever de confidencialidade, bem como

o direito do utente dos serviços de saúde "a ser informado pelo prestador dos cuidados de saúde sobre a sua situação, as alternativas possíveis de tratamento e a evolução provável do seu estado" (n. º 1 do artigo 7.º). Prevê-se ainda que "A informação deve ser transmitida de forma acessível, objetiva, completa e inteligível" (n. º 2). Só assim se logrará respeitar a dignidade, a liberdade, a autonomia dos utentes, condições essenciais para que os utentes possam exercer, de forma plena e efetiva, o seu direito fundamental de acesso à saúde na era da informação.

Do exposto, resulta claro que legislação portuguesa, em matéria de direitos dos utentes, tem evoluido e, o país continua a registar uma melhoria dos indicadores relativos aos direito à informação, aos resultados e à prevenção, por parte dos pacientes. Segundo o EHCI – *Euro Health Consumer Index* (classificação anual dos sistemas de saúde nacionais da Europa), Portugal, em 2017, situa-se na 14.ª posição, em um *ranking* de 35 países, a mesma de 2016 e após ter ocupado o 20.º lugar em 2015[30]. Porém, em matéria de direitos do utente, há ainda um longo caminho a percorrer e Portugal tem se preparado paulatinamente para a aplicação do Direito Europeu, sobretudo mediante a entrada em vigor de seu mais recente instrumento jurídico, o RGPD.

O RGPD enuncia vários direitos, nomeadamente o direito dos utentes terem acesso aos dados de saúde, dados de registro médicos e quaisquer intervenções ou tratamento realizados. Refere-se ainda à circunstância em que cada titular de dados, deverá ter o direito de conhecer e ser informado das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente aos eventuais tratamentos automáticos dos dados pessoais e, ao menos quando tiver por base a definição de perfis, das suas consequências[31].

Do exposto, resultam uma maior exigência no nível dos procedimentos a praticar pelo responsável dos tratamento dos dados de saúde, quer sejam hospitais, clínicas, centros de saúde etc, tais como: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimato, bloqueio ou eliminação de

[30] SNS-Serviço Nacional de Saúde. Disponível em: http://mkt.sns.gov.pt/vl/af370af3e-ba7fc3f594f6-9bca11b3d8595f21b6e6Ze0ePFSe.
[31] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, considerando 63.

dados desnecessários ou excessivos; portabilidade de seus dados pessoais para outro fornecedor de serviço ou produto; informação das entidades públicas e privadas com as quais o responsável realizou uso compartilhado de dados; informação sobre a faculdade de não fornecer o consentimento e sobre as consequências dessa negação; revogação do consentimento.

Por último, convém enaltecer que o responsável pelo tratamento de dados deverá informar de imediato a identidade de outros com os quais tenha compartilhado esses dados sobre o pedido de correção, de eliminação, de anonimização ou de bloqueio dos dados, para que repitam idêntico procedimento.

O RGPD, na realidade, responde com a figura do consentimento informado, alinhando-o como um dos fundamentos para a legitimidade do tratamento de dados pessoais. Nos termos do n. 1 do artigo 4. do RGPD, "O consentimento consiste em uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados, aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

Pode-se ainda extrair do RGPD que: o silêncio do paciente não constitui consentimento e o consentimento explícito é necessário para o tratamento de dados sensíveis (artigo n. 9.º); o responsável pelo tratamento deve poder demonstrar que o titular dos dados pessoais deu o consentimento para o seu tratamento (artigo n.º 7.º) e o titular dos dados deve ter a possibilidade de retirar o seu consentimento a qualquer momento, que deve ser tão fácil de retirar como de consentir (artigo n.º 7.º b); o consentimento pode ser dado, validando uma opção ao visitar um sítio Web na Internet; selecionando os parâmetros técnicos para os serviços da sociedade de informação e mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais[32].

No Código Deontológico da Ordem dos Médicos, o legislador português reforça no n. 1 do artigo 20 que "o consentimento do doente só é válido se este, no momento em que o dá, tiver capacidade de decidir livremente, se estiver na posse da informação relevante e se for dado na ausência de coações físicas ou morais". Relevante, portanto, é o intervalo de tempo que

[32] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, considerando 32.

deve ser respeitado, entre o esclarecimento e o consentimento, de modo a permitir ao doente refletir e aconselhar-se (n. 2). No mesmo sentido, o artigo n. 157 do Código Penal observa que o consentimento "só é eficaz quando o paciente tiver sido devidamente esclarecido sobre o diagnóstico e a índole, o alcance, a envergadura e as possíveis consequências da intervenção ou do tratamento, salvo se isso implicar a comunicação de circunstâncias que, ao serem conhecidas pelo paciente, poriam em perigo a sua vida ou seriam suscetíveis de lhe causar grave dano à saúde física ou psíquica."

Cabe ainda uma breve alusão ao direito à privacidade dos participantes em investigação científica, que não deve ser violada sem o consentimento informado, tal como defende o *International Committee of Medical Journal Editors* (ICMJE). Tanto os autores quanto os editores, em síntese, são responsáveis pela proteção dessa privacidade. Os autores da investigação devem fazer prova que os procedimentos seguidos foram avaliados por uma comissão de ética ou, na ausência desta, que os procedimentos estão em conformidade com a Declaração de Helsinque. Por sua vez, a aprovação de uma comissão de ética não iliba o editor do cumprimento da legislação em vigor. Em todo caso, na ausência do consentimento informado, as informações de natureza pessoal dos pacientes e dos participantes nos estudos a publicar, designadamente nomes, iniciais, ou números de hospitais, só devem ser publicadas em descrições escritas, fotografias ou genealogia se a informação for essencial para os fins científicos que se visa alcançar e se os mesmos forem de interesse público.

3.2. Na construção de um feixe protetivo no ordenamento jurídico brasileiro

Como se infere até aqui, trata-se de uma temática que flerta com outros aspectos, consistindo em um tema antigo com uma nova roupagem. No entanto, enquanto manifestação específica, exige resposta específica e igualmente inequívoca com fundamento na dignidade da pessoa humana, na autonomia informativa[33], com particular relevo para a sua multidimensionalidade, e no livre desenvolvimento da personalidade[34]. A grande novidade, de fato, se projeta a partir do enquandramento dos conflitos em um ambiente digital e, mais precisamente, em função da realidade factível de que os dados pessoais podem ser coletados, usados e abusados.

---

[33] LA CUEVA, Pablo Lucas Murillo de. *El derecho a la autodeterminación informativa. Temas clave de la Constitucion Española*. Madrid: Editorial Tecnos S.A., p. 38-39.

[34] Notabiliza-se a dicção constitucional que, no artigo 205 da CF/88, assegurou: "A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa para o exrcício da cidadania e sua qualificação para o trabalho."

Nesse sentido, sob o influxo de uma Constituição democraticamente promulgada, sobretudo em consequência do seu prodigioso catálogo de direitos e de garantias que se abre para a perspectiva de uma proteção multi-nível da pessoa humana, o Brasil desde 1988 tem erigido um sistema normativo que, em certa medida, é legatário das Cartas alemã[35] e portuguesa que, muito embora, não seja uma Carta digital, atualiza-se face a essa realidade de privacidade hipercontextualizada. De qualquer modo, afiança, protege, respeita e promove a centralidade da pessoa humana.

A propósito, a Constituição Federal de 1988, doravante CF/88, é uma aposta na democracia, no Estado Democrático de Direito, na dignidade da pessoa humana[36], na garantia dos direitos fundamentais e dos direitos humanos, na tolerância, no pluralismo, na responsabilidade, no solidarismo e nas múltiplas formas de exercício da cidadania plena, inclusive a digital. A Constituição trintenária, desse modo, enunciou a promessa de um processo democrático que pavimentaria o caminho para um país igualitário, sem discriminações de qualquer natureza e garantidor dos direitos humanos, estruturando-se a partir de um plexo de forças dramaticamente estabilizadas para oportunizar a emancipação e a proteção integral da pessoa humana[37], sendo, portanto, aplicável tanto no ambiente real quanto no digital.

Destaque-se, dessa maneira, a consagração do direito à saúde que, em uma conjugação com o direito à informação[38], perfaz a adequada moldura constitucional para o consentimento como tem sido tratado até aqui. Nesse aspecto, salienta-se que a doutrina brasileira, quando da introdução desse instituto no cenário nacional, enfatizou sua importância ao adotar a terminologia de consentimento informado, livre e esclarecido para, assim, realçar a ideia de anuência livre e consciente pautada no resguardo da autonomia em todos os momentos do processo de tomada de decisão.

---

[35] STARCK, Christian. *A proteção dos direitos fundamentais pelos tribunais e o papel da legislação na Alemanha*. In: Liber Amicorum Fausto de Quadros, vol. 1, Marcelo Rabelo de Sousa e Eduardo Vera-Cruz Pinto (Coord), 2016, p. 315-325.

[36] BARROSO, Luis Roberto. *Dignidade da pessoa humana no direito constitucional contemporâneo: a construção de um conceito jurídico à luz da jurisprudência mundial*. São Paulo: Fórum, 2013. p. 39; KLOEPFER, Michael. Vida e Dignidade da Pessoa Humana. In: Ingo Wolfgang Sarlet (Org.). Dimensões da Dignidade. Ensaios de Filosofia do Direito e Direito Constitucional, 2 ed, Porto Alegre: Livraria do Advogado Editora, 2009, p. 171 e ss.

[37] RODOTÀ, Stefano. *La rovoluione della dignità*. Napoli: La scuola di Pitagora editrice, 2013, p. 15.

[38] LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, 73. A CF/88 conjuga em especial os incisos IV, IX e XIV do artigo 5 com o teor do artigo 220 para a garantia do direito à informação e à comunicação.

Propício é o registro acerca do teor das resoluções do Conselho Nacional de Saúde-CNS que enaltecem a obrigatoriedade do consentimento nas pesquisas em seres humanos. A resolução 196 de 1996 afirmou para esse fim a cogência das regras sobre os comitês de ética, considerando os riscos e benefícios e submetendo-os à exigência de análise de protocolos de pesquisa em última instância pela Comissão Nacional de Ética em Pesquisa-CONEP instituída sob a forma colegiada e de natureza consultiva, normativa e independente. Em 2012 essa resolução foi atualizada pelo que dispõe a de número 466 que é o atual documento magno no que toca às pesquisas que envolvem seres humanos e, nesse sentido, disciplina temas como integridade da pesquisa que, em outras palavras, diz respeito ao modo como o pesquisador trata os dados coletados. Essa resolução dispõe ainda sobre os atuais desdobramentos da obrigatoriedade do consentimento.

No que concerne à digitalização, significativos esforços legislativos, doutrinários[39] e jurisprudenciais tem sido envidados para a regulação dos riscos e, assim, para o reconhecimento do direito à proteção dos dados sensíveis como direito fundamental autônomo, distinguindo-se, e.g., na esfera do âmbito de proteção as circunstâncias que envolvem sobretudo a teia de responsabilidade que afeta à ideia de compartilhamento e a sua titularidade.

Oportuno lembrar que, dentre a esfera da infraconstitucionalidade, há um *pool* legislativo que merece menção. À guisa de ilustração, os artigos 21 e 186 do Código Civil brasileiro tratam sobre a inviolabilidade da vida privada e sobre a base da responsabilidade civil por violação e por dano. Já o artigo 152 do diploma penal trata da inviolabilidade da correspondência, ressaltando-se o teor da Lei 12.737/2012 que introduziu a ideia de delitos informáticos que, apesar do assodaço como foi conduzido o processo legislativo e da enfatização dos ataques ao *hardware* em detrimento da proteção mais efetiva ao *software,* teve um caráter extremamente inovador à época.

Da seara consumeirista, por sua vez, além da nuclear construção do conceito de vulnerabilidade no ordenamento jurídico pátrio, deve ser sublinhada a contribuição no que

[39] SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. *O Direito ao "esquecimento" na sociedade da informação*. Porto Alegre: Livraria do Advogado, 2019, p. 23; RODRIGUES JÚNIOR. Otávio Luís. *Autonomia da vontade, autonomia privada e autodeterminação- notas sobre a evolução de um conceito na modernidade e na pós-modernidade*. In: Revista de Informação Legislativa. Brasília. N. 41. N. 163. Jul/Set 2004, p. 113-130.

afeta os artigos 43, 72 a 74 do Codigo de Defesa do Consumidor. Por outro lado, deve ser grifada a infeliz ausência de previsão de anuência do investigado no teor da Lei 12.037/2009 que previu a criação de bancos de perfil genético, particularmente em conjugação com o Decreto 7950/2013 que flagrantemente viola o inciso LXIII do artigo da CF/88. Igualmente sobressai a falta de previsão da anuência do cidadão com relação à inserção de seus dados no cadastro estruturado a partir da Lei 12.414/2011 e, finalmente, no que se refere à disponibilidade dos dados que compõem o Data-SUS.

Em rigor, nos termos da Lei 12.965 de 23 de abril de 2014, a despeito de não ser uma lei geral de proteção de dados, é que ocorreu o estabelecimento de uma base principiológica voltada para conjuntura advinda com a era digital. Segundo o artigo 3, a disciplina do uso da internet no Brasil tem os seguintes princípios: - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da CF/88; a proteção da privacidade; e a proteção dos dados pessoais. Conforme o artigo 6, na interpretação dessa Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e seus costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural. Do teor do artigo 7 depreende-se as normas sobre danos morais e materiais em caso de violação da intimidade e da vida privada. Em particular acerca da inviolabilidade e do sigilo do fluxo de comunicações e das comunicações armazenadas, há a previsão do direito ao não fornecimento a terceiros de dados pessoais mediante consentimento do usuário, à exclusão definitiva dos dados pessoais fornecidos à aplicação específica na internet, à publicidade e à clareza de eventuais políticas de uso dos provedores de conexão e de aplicações.

Nos termos dos artigos 10 e 11 é estruturada a base para a garantia do direito à proteção de dados no Brasil, remetendo à regulamentação efetuada pelo Decreto 8771/16. De modo geral, ao usuário são assegurados, dentre outros, os seguintes direitos[40]: - inviolabilidade da intimidade e da vida privada, a proteção e a indenização pelo dano material ou moral decorrente de sua violação nos domínios da internet, salvo por ordem judicial, na forma da lei; - inviolabilidade e sigilo de suas comunicações privadas e dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta

[40] Conferir no contexto alemão em: HOFFMANN, Christian; LUCH, Anika D.; SCHULZ, Sönke E.; BORCHERS, Kim Corinna. *Die digitale Dimension der Grundrechte- Das Grundgesetz im digitalen Zeitalter*. Baden-Baden: Nomos, 2015, p. 217.

Lei; A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados para a preservação da intimidade, da vida privada, da honra e da imagem das partes, direta ou indiretamente envolvidas[41].

No entanto, foi apenas em 2018, isto é, a reboque da entrada em vigência do RGPD, ou seja, mediante a sanção da Lei Geral de Proteção de Dados, doravante LGPD, que se tornou evidenciado a transparência como elemento central e, desta forma, de que todos os procedimentos envolvendo dados pessoais devam ser compatíveis com a finalidade da coleta e minimizados em uma política de uso racional, sobretudo em razão da sua perenidade. Outro aspecto notável foi o fortalecimento da proteção e a decorrente vedação de uso de dados sensíveis para fins discriminatórios independentemente do consentimento do usuário, especialmente face aos riscos de destruição, de divulgação e de acesso indevido em razão da estrutura aberta da internet. Desta feita, registros médicos não podem ser comercializados, sendo vedada a reutilização de dados sem o devido consentimento, restando essa possibildade apenas em caráter excepcional como de legítimo interesse que, na condição de conceito indeterminado, vai carecer de uma análise própria acerca da sua aplicabilidade prática, notadamente tendo em vista o veto presidencial em relação da criação de uma agência reguladora própria (Autoridade Nacional de Proteção de Dados- ANPD)[42].

A LGPD em nítida reafirmação da preponderância do consentimento como elemento crucial das relações no ambiente digital, em especial no que toca à proteção de dados sensíveis, reconheceu, dentre outros, os direitos de acesso, de retificação, de cancelamento, de exclusão, de oposição, de revogação da anuência. Além disso, reafirmou o direito à informação e de esclarecimento sobre a utilização de dados, enfatizando a ideia de titularidade na medida em que consagrou o direito à portabilidade. Impende relembrar a garantia do direito de pedido de revisão de decisão tomada com base em algoritmos e, nesse

[41] Disponivel em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 08 jan. 2018.

[42] Em 28 de dezembro de 2018 o presidente Michel Temer, por meio de medida provisória, instituiu a ANPD. A MP 869/18, atualmente em tramitação na Câmara dos Deputados, criou a ANPD como um órgão submetido à presidência da República, pertencente ao Executivo e formado por um conselho diretor de cinco membros indicados pelo presidente para mandato de quatro anos. Dentre outras, as principais atribuições da ANPD são: Criação de uma política nacional de de proteção de dados pessoais; garantir a privacidade desses dados; fiscalizar e aplicar sanções; promover campanhas de informação junto à população sobre as normas e as políticas públicas de proteção de dados pessoais; promover ações de cooperação com autoridades estrangeiras sobre esse tema; propor diretrizes estratégicas; elaborar relatórios anuais de avaliação da execução da política nacional de proteção de dados. De qualquer sorte, deve ser reforçado que a MP alterou parcialmente o Marco civil da Internet na medida em que abriu a possibilidade de pessoas jurídicas de direito privado controladas pelo poder político tratarem bancos de dados ultra relevantes como os dados sobre segurança pública, defesa nacional, segurança do Estado ou atividade de investigação e ou repressão penal.

sentido, a teia de responsabilização que envolve a segurança dos dados, gerando, e.g., a obrigação imediata de informar por meio de relatórios caso haja indícios de vazamento ou qualquer dano à estrutura de proteção. Igualmente relevante é a obrigatoriedade de novo consentimento em razão da necessidade de alteração de emprego dos dados, seja em razão da coleta, do tratamento ou da finalidade.

O consentimento, portanto, a partir da aplicação dessa legislação, deve estar inscrito em uma constelação de circunstâncias para ser pleno e válido que envolvem, dentre outros elementos outrora descritos, uma temporalidade estrita ao uso previamente informado e esclarecido, o qual tenha sido ampla e livremente objeto de deliberação de pessoa autônoma, importando em ressaltar os limites dessa categoria em um país que tristemente ainda expressa altas taxas de analfabetismo funcional e que passa por uma crise institucional grave. No entanto, surge, a partir daí outra mirada que, a despeito de sua relevância, não será objeto dessa investigação, resguardando-se, todavia, a adequação da qualidade e da quantidade de informação a ser prestada previamente como um pressuposto essencial.

4. Considerações finais

Importa acentuar que o ponto de partida para este estudo foram as dúvidas sobre a efetividade da garantia de proteção dos dados pessoais em saúde mediante emprego dos instrumentos jurídicos em vigor e, nessa medida, acerca das possibilidades de engendramento de uma cultura transfronteiriça cujo alcance oferecesse parâmetros para países como o Brasil que ainda podem ser considerados um tanto quanto neófitos nessa seara, sobretudo a partir das experiências européias e mais especificamente da portuguesa, de respeito pelos dados pessoais em geral, notadamente no que tange aos dados sensíveis e sempre enfatizando o consentimento informado como garantia primordial.

Verifica-se que os verdadeiros alicerces éticos e jurídico para a proteção da informação de saúde na internet já se encontram plasmados em instrumentos internacionais, tais como: Código de Nuremberg; Declaração Universal dos Direitos Humanos DUDH; Convenção Europeia dos Direitos Humanos; Declarações de Helsinque, Carta dos Direitos Fundamentais da União Europeia e Tratado de Lisboa. E consistem em intrumentos que vêm reconhecendo, ao longo dos séculos XX e XXI, a dignidade, a liberdade e a autonomia do ser humano em conformidade com os valores estruturantes da sociedade brasileira e portuguesa.

Entretanto, digno de nota foi que apenas com o Regulamento Geral de Proteção de Dados, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que a União Europeia veio uniformizar o regime de tratamento de dados, considerado como um requisito essencial para o bom funcionamento do Mercado Único, cujo impacto ao nível da proteção da privacidade dos titulares de dados, vai para além da União Europeia, alcançando países que intentam, dentre outras, manter as trocas econômicas.

Os esforços desenvolvidos tracejam pontos conclusivos circunscritos apenas ao fato de que indiscutivelmente foram lançadas as fundações para a edificação de uma cultura de proteção de dados pessoais no mundo, atingindo as estruturas normativas no Brasil e mais diretamente em Portugal. Dentre as alterações mais relevantes está o reconhecimento da autonomia, da liberdade, da dignidade, da privacidade e do livre desenvolvimento da personalidade como alicerces de qualquer sistema de proteção de dados pessoais, em particular no ambiente digital. Destaca-se, portanto, o valor inescusável do consentimento informado que deve ser considerado o fio condutor da proteção da pessoa humana e, mais especificamente, da sua autodeterminação que, em rigor, envolve a dimensão informativa.

Tudo visto, torna-se perceptível que o fortalecimento do consentimento informado como uma expressão livre, consciente e informada do sujeito de direito é o núcleo essencial para a proteção da informação de saúde na internet que evidentemente passa pela tentativa de uniformização do regime de tratamento de dados, cujo impacto ao nível da proteção da privacidade dos titulares de dados, vai para além da União Europeia.

Desse modo, o consentimento informado como forma de legitimar o tratamento de dados em saúde, o direito de oposição designadamente à utilização de dados pessoais para efeitos de definição de perfis; o direito de portabilidade dos dados de um prestador de serviços para outro e, a obrigação de os responsáveis pelo tratamento de dados fornecerem aos titulares dos dados, informações transparentes e de fácil acesso sobre o processamento dos seus dados, permite-nos observar que na atualidade estão sendo criados os critérios para a edificação de uma cultura de proteção de dados pessoais no Brasil e em Portugal.

Interessa tanto ao Brasil quanto a Portugal, face à vulnerabilização eminente, destarte, a conjugação de esforços que possam oferecer bases doutrinárias, jurisprudenciais e legislativas para a solução de conflitos vindouros a partir de elementos apropriados que, em

síntese, não flexibilizem as bases das conquistas dos sujeitos de direito, independemente do meio em que se encontrem, sobretudo a partir de uma proteção multinível que impeça retrocessos no âmbito de proteção dos direitos que perfazem a moldura de garantias inclusive no ambiente de *Big Data*.

Por fim, considera-se de exponencial relevância sublinhar a necessidade da adequação da informação previamente prestada quanto aos critérios de quantidade e de qualidade para a garantia dos direitos humanos e fundamentais dos usuários dos serviços de saúde no meio digital, particularmente no que toca à *gnose* a ser elaborada em razão do processo de deliberação.

5. Referências

AFINAL, quanta energia elétrica a internet utiliza para funcionar? *TECMUNDO*. Disponível em*:* <https://www.tecmundo.com.br/internet/104589-quanta-energia-eletrica-internet-utiliza-funcionar.htm> Acesso em: 17 jan. 2018.

AGAMBEN, Giorgio. *Lo abierto: el hombre y el animal*. Flavia Costa y Edgardo Castro (Trad). Buenos Aires: Adriana Hidalgo, 2006, p. 35.

ALMEIDA, Silvio Luiz de. *O que é racismo estrutural?* Belo Horizonte: Letramento, 2018, p. 56.

ASCENSÃO, José de Oliveira. *Estudos sobre direito da internet e da sociedade da informação*. Coimbra: Almedina, 2001, p. 264.

BARROSO, Luis Roberto. *Dignidade da pessoa humana no direito constitucional contemporâneo: a construção de um conceito jurídico à luz da jurisprudência mundial*. São Paulo: Fórum, 2013. p. 39**.**

BRÜGGEMEIER, Gert. *Protection of personality rights in the Law of delict/torts in Europe: mapping out paradigms*. In: BRÜGGEMEIER, Gert; CIACCHI, Aurelia Colombia; O'CALLAGHAN, Patrick. (Ed.). *Personality rights in european tort law*. Cambridge: Cambridge University Press, 2010.

BRUNO, Fernanda. *Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade*. Porto Alegre: Sulina, 2013, p. 123.

CANCELIER, Mikhail Vieira de Lorenzi. *O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro*. Sequencia (Florianópolis). N. 76. Ago. 2017. p. 213-240.

CASTELLS, Manuel. (1999). *A Era da Informação: economia, sociedade e cultura,* vol. 3. São Paulo: Paz e terra, p. 21.

CUKIER, Kenneth; MAYER-SCHÖNBERGER, Viktor. *Big Data: A Revolution that will transform how we live, work and think*. Boston, New York: Mariner Books, 2014, p. 176.

DEODATO, Sérgio. *A proteção dos dados pessoais de saúde*. Porto: Universidade Católica Portuguesa, 2017, p. 16.

HABBERMAS, Jürgen. *Um Ensaio sobre a Constituição da Europa*. Trad. Mrian Toldy; Teresa Toldy. Lisboa: Edições 70 Lda, 2012. Título original: Essay zur Verfassung Europus (2011), p.37.

HOFFMANN, Christian; LUCH, Anika D.; SCHULZ, Sönke E.; BORCHERS, Kim Corinna. *Die digitale Dimension der Grundrechte- Das Grundgesetz im digitalen Zeitalter*. Baden-Baden: Nomos, 2015, p. 217.

KLOEPFER, Michael. *Vida e Dignidade da Pessoa Humana*. In: Ingo Wolfgang Sarlet (Org.), Dimensões da Dignidade. Ensaios de Filosofia do Direito e Direito Constitucional, 2 ed, Porto Alegre: Livraria do Advogado Editora, 2009, p. 171 e ss.

LA CUEVA, Pablo Lucas Murillo de. *El derecho a la autodeterminación informativa*. *Temas clave de la Constitucion Española*. Madrid: Editorial Tecnos S.A., p. 38-39.

LEITE, Flávia Piva Almeida. *O Exercício da Liberdade de Expressão nas Redes Sociais e o Marco Civil da Internet*. In Revista de Direito Brasileiro, vol. 13, n. 06, 2016, p. 150.

LEONARDI, Marcel. *Tutela e privacidade na Internet*. São Paulo: Saraiva, 2012, 73.

LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2008, p 17.

LIMBERGER, Têmis. *O direito à intimidade na era da* informática: a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007, p. 231.

MARINONI, Luis Guilherme; MITIDIERO, Daniel; SARLET, Ingo Wolfgang. *Curso de Direito Constitucional*. São Paulo: Revista dos Tribunais, 2014, p. 434-435.

MARSDEN, C.T. *Net Neutrality: towards a Co-Regulatory Solutions*. Londres: Bloomsburry Academic, 2010, p. 36.

PUGLIANO, John. *Os robôs querem o seu emprego*. Edições Saída de Emergência. Portugal: Porto Salvo, 2018, p. 157.

RAMSAY, Iain. Consumer protection in the era of informational capitalism. In: WILHELMSSON, Thomas; TUOMINEM, Salla; e TUOMOCA, Heli (ed.) *Consumer law in the information society*. The Hague. Kluwer Law International, 2001, p. 45.

RODOTÀ, Stefano. *La rovoluione della dignità*. Napoli: La scuola di Pitagora editrice, 2013, p. 15.

RODRIGUES JÚNIOR. Otávio Luís. *Autonomia da vontade, autonomia privada e autodeterminação- notas sobre a evolução de um conceito na modernidade e na pós-modernidade*. In: Revista de Informação Legislativa. Brasília. N. 41. N. 163. Jul/Set 2004, p. 113-130.

SANTAELLA, Lucia. *Linguagens líquidas na era da mobilidade*. São Paulo: Paulus, 2011, p. 178.

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M. *O Direito ao "esquecimento" na sociedade da informação*. Porto Alegre: Livraria do Advogado, 2019, p. 23.

SCHMIDT, Eric – COHEN, Jared. *The New Digital Age: Reshaping the Future of People, Nations and Business*. London: John Murray, 2014, p. 15.

STARCK, Christian. *A proteção dos direitos fundamentais pelos tribunais e o papel da legislação na Alemanha*. In: Liber Amicorum Fausto de Quadros, vol. 1, Marcelo Rabelo de Sousa e Eduardo Vera-Cruz Pinto (Coord), 2016, p. 315-325.

STATZEL, Sophie. *Cybersupremacy: The new Face and Form of white Supremacy Activism*. In: Digital Media and Democracy: Tactics in hard Times. Megan Boler(Edit.). Cambridge: MIT Press, 2008, p. 409.

SUNSTEIN, Cass R. *Republic: divided democracy in the age of social media*. New Jersey: Princeton University Press, 2017, p. 138.

THE Economist. LinkedUp. Disponível em: <http://www.economist.com/news/business_and_finance/21700605_it_one_most_expensive_tech_deals_history_it-may_not_be_smartest_making_sense>. Acesso em: 03 jan. 2018

THE Economist. *The world's most valuable resource is no longer oil, but data***.** Disponível em <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 01 jun.2018.

civilistica.com

Recebido em: 27.10.2018
Aprovado em:
11.2.2019 (1º parecer)
11.2.2019 (2º parecer)

Como citar: SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Civilistica.com**. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: <http://civilistica.com/o-consentimento-informado-e-a-protecao/>. Data de acesso.