X ENCONTRO INTERNACIONAL DO CONPEDI VALÊNCIA – ESPANHA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

AIRES JOSE ROVER

FERNANDO GALINDO AYUDA

ADRIAN TODOLI SIGNES

D598
Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/2020
Coordenadores: Aires José Rover; Fernando Galindo Ayuda; Adrian Todoli Signe – Florianópolis: CONPEDI, 2020 / Valência: Tirant lo blanch, 2020.

Inclui bibliografia
ISBN: 978-65-5648-003-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Crise do Estado Social

1. Direito – Estudo e ensino (Pós-graduação) – Congressos Nacionais. 2. Assistência. 3. Isonomia. X Encontro Internacional do CONPEDI Valência – Espanha (10:2019 :Valência, Espanha).

CDU: 34

X ENCONTRO INTERNACIONAL DO CONPEDI VALÊNCIA – ESPANHA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

O X ENCONTRO INTERNACIONAL DO CONPEDI VALÊNCIA – ESPANHA mostrou que os temas relacionados às novas tecnologias estão cada vez mais inseridos na realidade jurídica brasileira e mundial. Diversos fenômenos do cenário digital foram abordados ao longo dos trabalhos e demonstraram que a busca por soluções nessa esfera só pode ser pensada de forma multidisciplinar.

Assim, vejamos as principais temáticas tratadas nos artigos, em sua sequência de apresentação no sumário e apresentação no GT.

O primeiro artigo tratou da governança ambiental e a necessária participação social nesse processo; o seguinte, a utilização de drones em serviços de entrega, sofrendo com falta de regulação e uma visão burocrática do serviço; em seguida, a discussão de casos de dados sensíveis de pacientes sendo expostos em redes sociais e a fundamental conscientização da existência da autodeterminação já definida em lei; a importância da teoria do risco na responsabilidade civil dos novos atores digitais; tratou do conceito de armas autônomas e a precária situação de regular seu uso pelos estados; a difícil comunicação entre seres humanos e robôs dotados de inteligência artificial a partir da teoria de Luhmann; a transformação e mesmo morte do modelo clássico de contratos com o crescente uso do blockchain; os limites legais ao uso de dados pessoais pelo big data e os reflexos na livre concorrência e no desenvolvimento socioeconômico; uma comparação entre as normas jurídicas de proteção de dados na Europa e no Brasil; o artigo que tratou de inteligência artificial e direito buscou fazer uma revisão sistemática da literatura relativa ao seu uso em situações de resolução de conflitos on-line.

Com esses estudos de excelência os coordenadores desse grupo de trabalho convidam a todos para ler na integra os artigos, dando prosseguimento ao debate de temáticas inovadoras e centrais no mundo atual.

Prof. Dr. Aires José Rover - UFSC

Prof. Dr. Fernando Galindo Ayuda - Universidad de Zaragoza

Prof. Dr. Adrian Todoli Signes - Universidad de Valencia

O USO DE DADOS SENSÍVEIS DE PACIENTES NAS REDES SOCIAIS E A LGPD

THE USAGE OF SENSITIVE DATA OF PATIENTS IN SOCIAL NETWORKS AND THE BRAZILIAN GENERAL DATA PROTECTION ACT

Cinthia Obladen de Almendra Freitas [1]
Jussara Maria Leal De Meirelles [2]

Resumo

A Internet, a facilidade de coleta e armazenamento de dados, a informatização de processos e empresas, a evolução da comunicação e da transmissão de conteúdo, têm demonstrado que se vive numa sociedade da exposição. Importa analisar o uso de dados sensíveis de pacientes em redes sociais, frente à Lei Geral de Proteção de Dados (LGPD) - Lei no 13.709, de 14 de agosto de 2018. O artigo, resultado de projeto de pesquisa, segue método dedutivo, exploratório e descritivo para relacionar, criticamente, o uso de dados sensíveis de pacientes em redes sociais, com o direito à privacidade e a LGPD.

Palavras-chave: Sociedades, Novas tecnologias, Direito à privacidade, Lgpd, Dados sensíveis

Abstract/Resumen/Résumé

The Internet, the ease of data collection and storage, the computerization of processes and companies, the evolution of communication and the transmission of content, have demonstrated that we live in an exhibition society. It is important to analyze the use of patients' sensitive data in social networks, faced to the Brazilian General Data Protection Act (LGPD) - Act 13709 of August 14, 2018. The article, as result of a research project, follows a deductive method, exploratory and descriptive study to critically relate the use of patients' sensitive data in social networks with the right to privacy and the LGPD.

Keywords/Palabras-claves/Mots-clés: Societies, New technologies, Right to privacy, Brazilian general data protection act, Sensitive data

[1] Doutora em Informática (PUCPR). Professora Titular.Programa de Pós-Graduação em Direito Econômico e Socioambiental (Mestrado e Doutorado) da PUCPR - Curitiba-PR, Brasil

[2] Doutora em Direito das Relações Sociais (UFPR). Pós-Doutorado no Centro de Direito Biomédico da Universidade de Coimbra. Professora Titular. PPGDireito e PPGBioética - PUCPR - Brasil.

1. INTRODUÇÃO

Privacidade é assunto antigo. O trabalho de Warren e Brandeis já pontuava em 1890 (WARREN; BRADEIS, 1890), época em que nem se falava em computadores, celulares, Internet e redes sociais, que os indivíduos tinham e sempre terão direito à proteção sobre a pessoa e a propriedade sendo, portanto, a discussão sobre privacidade muito antiga.

Em estudo empírico realizado por Liccardi *et al.* (2013, p. 9), foram analisadas as Políticas de Privacidade de 528.433 aplicativos, o que representava 88% da *playstore* para dispositivos móveis com sistema Android, e os autores constataram que apenas 6,6% destes aplicativos possuíam uma Política de Privacidade disponível na *playstore*, ou seja, antes de realizar a instalação de cada um dos aplicativos. Os autores observaram que isto representava, consequentemente, que mais de 93% dos aplicativos não explicavam claramente como usavam os dados pessoais disponíveis nos celulares ou coletados no decorrer do uso dos aplicativos (LICCARDI *et al.*, 2013, p. 10). O objetivo da pesquisa realizada era medir o que foi denominado pelos autores de "pontuação de sensibilidade" (*sensitivity score*) para representar o número de ocorrências de permissões que leem dados pessoais dos usuários juntamente com a capacidade de transmitir os dados coletados quando os dispositivos estavam conectados à Internet. Assim, descobriram que 54% dos aplicativos não acessavam nenhum dado pessoal, porém os 46% restantes coletavam entre 1 e 20 permissões sensíveis e tinham a capacidade de transmitir dados para fora do celular (LICCARDI *et al.*, 2013, p. 7-9). São exemplos de permissões sensíveis coletar dados sobre: localização (GPS ou baseado em rede), contatos, perfil de uso, registros confidenciais, favoritos e histórico da web, calendário, *social stream*[1], eventos da agenda do Gmail, mensagens de texto (SMS[2] ou MMS[3]), mensagens instantâneas, marcadores e histórico da *web*, lista de contatos, *status* e identificadores do dispositivo móvel, lista de registro de chamadas, entre outros.

Duas categorias de aplicativos chamam a atenção no estudo de Liccardi *et al.* (2013, p. 15): *Health & Fitness* e *Medical*; sendo o número total de aplicativos analisados na categoria *Health & Fitness* igual a 13.487 e na categoria *Medical* igual a 6.347. Os autores

[1] *Social Stream* é um aplicativo inovador que permite agregar todos os seus feeds de redes sociais em um único fluxo de rede ou criar um único feed para vários perfis de redes sociais. Isso tornará os fluxos de redes sociais mais interativos e fáceis de analisar, aumentando assim o tráfego na Web e aumentando o engajamento de mídias sociais.

[2] SMS (do inglês *Short Message Service*) é um serviço de mensagens curtas disponível em telefones celulares digitais que permite o envio deste tipo de mensagem entre estes equipamentos e entre outros dispositivos de mão, e até entre telefones fixos.

[3] MMS (do inglês *Multimedia MessagingService*) é um serviço que permite aos *smartphones* trocarem mensagens contendo imagens, vídeos, sons, lista de contato e dados de localização.

concluem que para tais categorias, considerando os aplicativos pagos, a "pontuação de sensibilidade" (*sensitivity score*) é 2,28 e 1,53, respectivamente para *Health & Fitness* e *Medical*, sendo a média geral entre as 31 categorias de aplicativos analisados igual a 1,53 (LICCARDI *et al.* (2013, p. 20-21). Já para os aplicativos gratuitos, a "pontuação de sensibilidade" (*sensitivity score*) é 2,76 e 2,86, respectivamente para *Health & Fitness* e *Medical*, sendo a média geral entre as 31 categorias de aplicativos analisados igual a 2,72 (LICCARDI *et al.* (2013, p. 20-21). Os autores consideram que aplicativos com *sensitivity score* > 1 são aqueles que solicitam permissões sensíveis e de Internet.

Portanto, observa-se que as categorias: *Health & Fitness* e *Medical*; apresentam "pontuação de sensibilidade" (*sensitivity score*) > 1 tanto entre os aplicativos pagos quanto entre os aplicativos gratuitos e, ainda, que os aplicativos gratuitos coletavam mais permissões sensíveis e tem a capacidade de transmitir dados para fora do celular. O que é altamente preocupante no cenário da sociedade de informação e exposição em que se vive e, mesmo sem perceber, os dados estão sendo coletados e utilizados.

A Internet, a informatização de processos e empresas, a facilidade de coleta e armazenamento barato de dados nos mais diferentes formatos e tamanhos, concomitantemente com a evolução da comunicação e da transmissão de conteúdo, vem gerando tantas transformações que termos como Inteligência Artificial, Aprendizagem de Máquina, Aprendizagem Profunda, Computação Ubíqua, Computação Pervasiva, *Big Data*, Sociedade de Algoritmos, Sociedade Transparente, Sociedade da Exposição, Sociedade de Controle e muitos outros se tornaram parte do cotidiano. Vive-se uma geração em que a Informática pode desenvolver e aplicar praticamente qualquer algoritmo baseado em dados. Vive-se a "obesidade" de dados, visto que dados são coletados mesmo sem finalidade definida, o que resulta em exageros e falta de privacidade. É muito difícil para qualquer usuário da Internet saber onde, quando e para que são ou foram coletados seus dados, onde estão armazenados e como estão sendo processados ou tratados.

A partir desta contextualização, tem-se que privacidade e proteção de dados constituem temas recorrentes e continuam atuais. E, no Brasil, são temas atualíssimos a partir do advento da Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709, de 14 de agosto de 2018. Nesse sentido, o confronto entre o Direito e o uso de dados sensíveis de pacientes em redes sociais, frente ao marco legal recém estabelecido, é inevitável para uma melhor compreensão da sociedade da exposição. Assim, o artigo é resultado de projeto de pesquisa e segue método dedutivo para relacionar o uso de dados sensíveis de pacientes com o direito à privacidade, em sua esfera mais íntima, com o que preconiza a LGPD, estabelecendo uma

crítica ao uso dos dados sensíveis de pacientes em redes sociais. A pesquisa tem caráter explicativo, passando pelas fases da pesquisa exploratória e descritiva.

2. O DIREITO À PRIVACIDADE E DADOS SENSÍVEIS

Mark Zuckerberg, fundador do Facebook, declarou em 2010 que a abertura e o compartilhamento de dados pessoais corresponderiam a uma evolução de uma "norma social"[4] (JOHNSON, 2010, p. 01), fazendo-se valer de interesse pela mudança de costumes sociais que são entendidos e aceitos como normais no que tange ao uso de dados pessoais. Eis aqui o debate entre o entendimento de uma norma jurídica que tutela a privacidade e os dados pessoais frente aos riscos existentes nas redes sociais, e a "norma social" mencionada por Zuckerberg, a qual segundo ele evolui ao longo do tempo, significando que os padrões de privacidade devem ser mais elásticos e dinâmicos, quando o interesse é coletar, tratar, compartilhar dados pessoais em redes sociais.

Indo ainda mais longe no tempo, a obra "*The right to privacy*" de Warren e Brandeis, de 1890, previa que os recintos sagrados da vida privada e doméstica haviam sido invadidos pela tecnologia da época, ou seja, as fotografias instantâneas que poderiam ser capturadas por qualquer pessoa e publicadas nos jornais de qualquer cidade, de modo que a solidão e a privacidade se tornaram mais essenciais para ao indivíduo. Os autores ponderam que as empresas modernas e as invenções, por meio de invasões na privacidade alheia, sujeitam o indivíduo a dores e aflições mentais muito maiores do que poderiam ser infligidas por meras lesões corporais (WARREN; BRANDEIS, 1890, p. 196).[5]

Cabe, portanto, considerando o reconhecimento dos direitos da personalidade no ambiente de constitucionalização do Direito Civil brasileiro[6], retomar a Teoria dos Círculos

[4] Texto original: "*People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people (...). That social norm is just something that has evolved over time".* (Tradução livre: "As pessoas realmente se sentiram confortáveis não apenas compartilhando mais informações e tipos diferentes, mas mais abertamente e com mais pessoas (...). Essa norma social é apenas algo que evoluiu ao longo do tempo").

[5] Texto original: *"The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury".* (Tradução livre: "A intensidade e a complexidade da vida, inerentes à civilização avançada, tornaram necessária alguma retirada do mundo, e o homem, sob a influência refinada da cultura, tornou-se mais sensível à publicidade, de modo que a solidão e a privacidade se tornaram mais essenciais para o indivíduo; mas a empresa moderna e a invenção, através de invasões em sua privacidade, sujeitaram-no a dores e aflições mentais muito maiores do que poderiam ser infligidas por meras lesões corporais").

[6] Constituição Federal – art. 1º, inciso III: a dignidade da pessoa humana (BRASIL, 1988); Constituição Federal – art. 5º, inciso X – "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988); Código Civil –

Concêntricos da Esfera da Vida Privada ou Teoria das Esferas da Personalidade *(Sphärentheorie)*, formulada em 1953 pelo jurista alemão Heinrich Hubmann e revisitada por Heinrich Henkel em 1957, também jurista alemão. A referida Teoria menciona que a vida privada do ser humano é composta por 3 círculos concêntricos, a saber: privacidade ou esfera privada (esfera externa), intimidade ou confidência (esfera intermediária) e segredo (esfera íntima) (DI FIORI, 2012., p. 2) (SZANIAWSKI, 2005) (NASCIMENTO, 2009, p. 26).

A privacidade é a esfera mais externa, na qual as relações interpessoais são superficiais (NASCIMENTO, 2009, p. 26) e, portanto, os dados aqui expostos ou divulgados devem ser somente os dados que possam ser classificados como públicos, visto não existir detalhamento sobre a vida das pessoas. Aqui se destaca o interesse público, pelo qual se tornam relevantes aspectos da vida privada que possam ser expressos, à sociedade, por meio de dados públicos. Não há invasão de aspectos íntimos, muito menos ligados à esfera do segredo.

A esfera intermediária, também denominada de intimidade, engloba aspectos da vida privada representados pelos dados pessoais e destina-se a proteger a esfera íntima da vida privada, mas não a esfera do segredo. Assim, tem-se que "a esfera íntima protege a pessoa inteiramente, ficando a mesma intocável aos olhos e ouvidos do público" (SZANIAWSKI, 2005, p. 357-358). Nesta esfera deve-se proteger o sigilo domiciliar, profissional e, por exemplo, comunicações telemáticas. Esta esfera engloba dados mais restritos do indivíduo, em comparação à camada externa (privacidade ou esfera privada). Aqui são compartilhados dados com poucas pessoas, a exemplo do ambiente familiar, amigos mais íntimos ou ambiente profissional por necessidade (DI FIORI, 2012, p. 4).

E por fim, tem-se a esfera do segredo, a qual constitui o conjunto de dados mais secretos sobre uma pessoa. A pessoa não deseja ver exposto ou compartilhado este conjunto de dados (DI FIORI, 2012, p. 4). E é nesta esfera que se encontram os dados sensíveis.

Bastos e Martins (1989, p. 63) conceituam o que é a privacidade:

> Faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

---

artigo 11, que preconiza que "... os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária" (BRASIL, 2002); Código Civil – artigo 21, "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma." (BRASIL, 2002).

Nota-se que a liberdade de expressão e a privacidade estão interligadas, não podendo uma ultrapassar os limites da outra, ponto este que deve ser sempre analisado, principalmente, na Internet, uma vez que nunca se pode querer publicar algo sobre a égide da liberdade de expressão sem deixar de analisar a privacidade dos envolvidos, internautas ou não.

Para Hughes (1993, p. 1) privacidade nada mais é do que se ter a escolha de selecionar para quem se deseja divulgar dados pessoais, ou seja, privacidade é o poder de se revelar ao mundo seletivamente:

> *Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world*[7].

De acordo com a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, em 14 de agosto de 2018, art. 5º, inciso II, dado pessoal sensível é "dado pessoal sobre a 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, 2018).

São os dados que caracterizam elementos que o indivíduo não gostaria de compartilhar com as demais pessoas ou com qualquer pessoa e, que além disto, podem gerar um alto risco de exposição na sua vida pessoal, social ou profissional. São os dados que compõem a esfera do segredo. Como exemplos: ao se cadastrar para ter acesso a um edifício privado ou público, normalmente, o indivíduo fornece, além do nome, RG ou CPF, uma foto (face – dado biométrico) e/ou impressão digital (dado biométrico); ao realizar exames médicos em uma clínica ou laboratório, a empresa reúne um conjunto de dados sobre a saúde e doenças pré-existentes, formando um histórico dos exames já realizados, dos médicos consultados e do plano de saúde; ao se cadastrar em um *site* ou agência de empregos, a empresa pode solicitar dados sobre sua religião, sobre a filiação ou não a sindicatos ou partido político, entre outros.

Neste cenário, o Código Civil também prevê proteção sobre a imagem da pessoa natural (BRASIL, 2002):

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a

[7] Tradução livre: "A privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é segredo. Um assunto privado é algo que ninguém quer que o mundo inteiro saiba, mas um assunto secreto é algo que não se quer que qualquer pessoa saiba. Privacidade é o poder de se revelar seletivamente para o mundo".

> boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
> Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.

Questiona-se, tomando-se as considerações apresentadas, se a privacidade está sendo deixada de lado pelos usuários da Internet frente ao uso, por exemplo, de aplicativos gratuitos, como descrito na Introdução do artigo. Ou será que os usuários temem o julgamento das demais pessoais caso não participem ou não se façam presentes nas redes sociais por meio de comentários, postagens, 'curtidas', como bem relata Dal Bello (2011, p. 6): "*As pressões de ser alguém, de ser único, levam ao aparecimento de novos sofrimentos íntimos: o indivíduo moderno teme fracassar no imperioso esforço de delimitar sua singularidade.*" A sociedade atualmente está mais preocupada com que os outros irão pensar do que em sua própria segurança; é mais importante 'parecer ser' do que o próprio 'ser'.

Considerando tais pontos é importante destacar os riscos aos quais os usuários estão expostos devido a essa 'necessidade' de se mostrar a todo custo. Tal exposição é causada justamente pelo fato de o usuário não saber utilizar as ferramentas tecnológicas e, também, por não se dar conta do poder que as redes sociais possuem, inferindo-se cautela com o que ali se posta e veicula.

Nove anos já se passaram da declaração dada por Zuckerberg e a discussão continua atual. De 1890 aos dias atuais, mais de 120 anos já passaram e a discussão sobre direito à privacidade e proteção de dados ainda é pertinente. Contados a partir de 1953, já passaram 67 anos e a Teoria da dos Círculos Concêntricos da Esfera da Vida Privada ou Teoria das Esferas da Personalidade *(Sphärentheorie)* pode ser revisitada sob a ótica dos dados públicos, pessoais e sensíveis.

Os riscos e vulnerabilidades a que estão expostos os usuários da Internet e de redes sociais por meio do desconhecimento sobre quais dados são coletados, como são tratados e armazenados ou, ainda, se há transferência e compartilhamento de dados entre parceiros comerciais, continua uma incógnita para cada titular de dados. Portanto, cabe ao Direito tutelar os dados pessoais e criar instrumentos legais que garantam, efetiva e eficazmente, o controle sobre o uso de dados pessoais e sensíveis.

Entende-se que a concepção dos direitos à vida privada e à intimidade deve ser dinâmica, flexível, de forma a acompanhar a evolução humana, seja ela social, tecnológica ou cultural. Porém, caberá ao indivíduo estabelecer o grau de dinamicidade e elasticidade que permitirá às suas esferas e, por consequência, aos seus dados. Não mais ditará a coleta e o tratamento de dados pessoais, nem mesmo valerá como legítimo interesse (artigo 10 da

LGPD) ou finalidade (art. 6º da LGPD) o interesse econômico sobre os dados (BRASIL, 2018).

3. REDES SOCIAIS E A EXPOSIÇÃO DE DADOS DE PACIENTES

Como apresentado a seguir, as redes sociais têm grande relevância na sociedade contemporânea, informacional e tecnológica, estando cada vez mais presente no cotidiano das pessoas. Dessa forma, o estudo foi levado a analisar o uso dos dados sensíveis de pacientes em redes sociais contextualizado sob a ótica da Lei Geral de Proteção de Dados (LGPD) frente à questão da exposição dos usuários de tais redes.

3.1 A Exposição nas Redes Sociais

As relações que as pessoas desenvolvem durante a vida constituem a sua inserção na sociedade. No entanto, nas redes sociais essa relação com os demais é o que vai formando a rede. As redes sociais, segundo Marteleto (2001, p. 72), são "um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados."

Devido à dinâmica que as redes possuem, acabam funcionando como espaços para compartilhamento de informação e de conhecimento onde pessoas com os mesmos objetivos trocam experiências. Como mesmo relata Capra (2002, p. 267):

> Na era da informação – na qual vivemos – as funções e processos sociais organizam-se cada vez mais em torno de redes. Quer se trate das grandes empresas, do mercado financeiro, dos meios de comunicação ou das novas ONGs globais, constatamos que a organização em rede se tornou um fenômeno social importante e uma fonte crítica de poder.

As redes são um coletivo onde a dinâmica facilita e por si própria representa o relacionamento de pessoas, possibilitando diversos usos e interações. Essa conexão entre as pessoas de forma mais fácil, se deu a partir da década de 90, quando do surgimento da Internet e do desenvolvimento das Tecnologias de Informação e Comunicação (TIC).

Como bem destacado por Recuero (2009), a Internet trouxe inúmeras mudanças para a sociedade, sendo a mais significativa delas a possibilidade de expressão e sociabilização, ou seja, torna sociável a comunicação por meio das novas tecnologias, proporcionando, então, comunicação direta e interação fortemente ativa com os demais usuários. E, ainda, descreve que a rede "é uma metáfora para observar os padrões de conexão de um grupo social, a partir das conexões estabelecidas entre os diversos atores" (RECUERO, 2009, p. 24).

Informação e conhecimento são palavras-chave que estão inseridas e agregadas às redes sociais, palavras que representam ações que se dão por meio das interações que ocorrem na rede. Desta forma, o usuário tem a possibilidade, e muitas vezes a necessidade, de compartilhar conteúdos com os demais usuários na rede. Além disso, a rápida mobilidade e velocidade de propagação de informações é outro ponto relevante das redes sociais.

Desse modo, entende-se que uma rede social tem como principais objetivos: o relacionamento, a comunicação e o compartilhamento de informações; constitui-se, portanto, uma ferramenta extremamente poderosa. Nesse contexto, a informação é o elemento mais importante e vital para a existência e, também, sobrevivência das redes sociais. Recuero (2005, p. 5) afirma que "... a análise estrutural das redes sociais procura focar na interação como primado fundamental do estabelecimento das relações sociais entre os agentes humanos, que originarão as redes sociais, tanto no mundo concreto, quanto no mundo virtual". Para tal, tem-se que as redes sociais são um meio de comunicação que aproxima e facilita o contato entre as pessoas, como afirma Marteleto (2001, p. 72):

> As Redes Sociais representam um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados. A questão central das redes é a valorização dos elos informais e das relações, em detrimento das estruturas hierárquicas. As redes sociais são exatamente as relações entre os indivíduos na comunicação mediada por computador. Esses sistemas funcionam através da interação social, buscando conectar pessoas e proporcionar sua comunicação.

Freitas (2015, p.78) aponta que "o excesso de informação se mostra atrelado ao excesso de exposição, exposição essa sem limites de cada indivíduo de maneira a refletir seus gostos, modo de vida, interesses, amigos, pensamentos e atitudes", relacionando a exposição com o excesso de informação disponibilizada e divulgada na Internet e, mais especificamente, pelas redes sociais.

A denominada sociedade de exposição trata do conjunto de pessoas que pouco se importa com a segurança do que é postado, veiculado e compartilhado na Internet, deixando de lado questões relacionadas à privacidade e à intimidade. Busca-se entender quais os motivos proporcionam tal uso da Internet e das redes sociais. Uma entre muitas razões pode estar relacionada ao querer, a qualquer preço, publicar e compartilhar conteúdo com os demais para que seja 'reconhecido' dentro da rede. Em uma pesquisa realizada pela Hi-Midia em parceria com a M. Sense, mostra para um conjunto de 484 pessoas entrevistadas que 50% dos usuários de Facebook se incomodam em receber *posts* irrelevantes e 40% dos usuários de Facebook sentem suas informações expostas (CAVALCANTI, 2013).

Recuero (2009, p. 121) aponta que a estrutura da rede social é o elemento "cuja principal característica é a exposição pública da rede dos atores, que permite mais facilmente divisar a diferença entre esse tipo de site e outras formas de comunicação mediada pelo computador".

A sociedade de exposição é, portanto, aquela que faz da Internet meio e fim, sendo que a exposição nasce a partir do instante em que o usuário começa a utilizar num primeiro momento a Internet e, posteriormente, as redes sociais.

3.2 A Exposição de Dados Sensíveis de Pacientes

A exposição de dados sensíveis de pacientes é inicialmente um tema redundante, visto que dados de pacientes sempre são sensíveis e, portanto, carecem de proteção naturalmente. Mas como mostrado a seguir, nem sempre os profissionais da área da saúde ou as empresas de Tecnologia da Informação e Comunicação (TIC), no desejo de expor ou coletar e tratar dados, estão atentos às consequências decorrentes do uso dos dados, a exemplo de imagens de pacientes e de seus problemas de saúde.

Caires *et al.* (2015, p. 255) explicam que, ao estar internado, o paciente se encontra em situação de extrema fragilidade, na qual muitas vezes precisa de cuidados que invadem sua intimidade. Afirmam os autores que "os pacientes enfrentam a hospitalização como um fator de despersonalização, pois reconhecem a dificuldade em manter sua identidade, intimidade e privacidade". E a observação da prática do cuidado do paciente revela "a falta de preocupação com a exposição corporal em muitas situações. Essa pessoa, que deve ser percebida como sujeito do cuidado, torna-se um objeto, perdendo sua identidade". Seguem, os autores, explicando que a exposição do corpo do paciente no momento do atendimento médico-hospitalar associada ao uso constante de celulares com câmera fotográfica, por muitos profissionais de saúde, facilita a captura e a reprodução de imagens de pacientes, principalmente, de pacientes com comprometimento do nível de consciência (Caires *et al.*, 2015, p. 256).

Para avaliar o nível de conhecimento dos profissionais de saúde quanto à captura e reprodução de imagens de pacientes em ambiente hospitalar, CAIRES *et al.* (2015, p. 256) avaliaram do universo de 2.590 profissionais, do Hospital da Universidade Federal de São Paulo, entre fevereiro e julho de 2013, uma amostra de 360 questionários (tendo o estudo um intervalo de confiança de 95% com erro de 5%). Os resultados demostraram que (Caires *et al.*, 2015, p. 256-258):

- Dos 360 profissionais de saúde entrevistados, houve um predomínio de 72,8% do sexo feminino, 89,7% tinham idade ≥ 40 anos, 31,4% eram enfermeiros, 36,7% relataram tempo de experiência profissional de 1 a 3 anos, e em relação ao local de trabalho no hospital, 43,0% trabalhavam em unidades de internação;
- 81,3% dos entrevistados declarou ter presenciado outro profissional de saúde fazendo imagens de pacientes, 9,7% dos quais haviam visto uma vez, 23,3% de duas a quatro vezes, 48,3% mais de quatro vezes, 5,3% relataram não lembrar, e 13,3% não eram testemunhas deste tipo de situação;
- Quando questionados se o profissional havia fotografado ou filmado pacientes no ano anterior ao da pesquisa, 57,8% responderam que sim e 71,1% afirmaram não ter fotografado ou filmado alguém que estivesse inconsciente;
- Entre os profissionais que responderam positivamente por terem capturado imagens (n = 147), a maioria relatou ter solicitado autorização verbal (61,2%) e a minoria solicitou autorização por escrito (10,9%);
- Dos 147 participantes que afirmaram ter feito imagens, 41,5% (n = 61) usaram para a apresentação de casos clínicos e estudos, 12,2% (n = 18) mostraram para amigos e parentes fora do trabalho, e 0,7% (n = 1) publicou em redes sociais.

CAIRES *et al.* (2015, p. 259) consideraram ainda a formação das pessoas e o tempo de trabalho, concluindo que técnicos de enfermagem e enfermeiros(as) com curso superior, bem como profissionais com maior tempo de experiência, realizam a captura e reprodução de imagens com menor frequência. Residentes das diversas áreas da saúde formaram a categoria que mais capturava e reproduzia imagens, apresentando menor conhecimento sobre os itens previstos na Constituição Federal, no Código Civil e no Código Penal sobre Direito de Imagem.

Carvalhal *et al.* (2017, p. 40) afirmam que "o direito à privacidade dos dados médicos garante ao indivíduo a manutenção das informações a seu respeito e seus problemas de saúde inacessíveis a outros indivíduos". De modo que, "toda informação decorrente de interações médicas é considerada confidencial, e o acesso a ela deve ser protegido". Os autores alertam que "a violação da privacidade de informações médicas pode afetar diretamente a vida de qualquer indivíduo, gerando consequências práticas", a exemplo de: percepção de terceiros sobre a expectativa de vida de uma pessoa ou profissional, possibilidade de desenvolvimento de certas doenças ou incapacidades, situações de paternidade ou de maternidade, existência de

doenças graves (por exemplo, psiquiátricas), uso de drogas ou medicamentos, lembrando que dados sobre opções sexuais podem gerar discriminação, com possíveis efeitos prejudiciais ao paciente tanto no campo pessoal quanto no campo social. Os autores concluem pela "atenção e educação contínuas de profissionais da área da saúde e de todos aqueles envolvidos com aquisição, uso e armazenamento de dados relativos à saúde de pacientes" (CARVALHAL *et al.*, 2017, p. 42-43).

Chiavegatto Filho (2015, p. 327) discute o uso de *Big Data* em saúde no Brasil, apontando a possibilidade do uso integrado do prontuário eletrônico do paciente (PEP), que consiste no acesso remoto de prontuários por todos os estabelecimentos de saúde. O autor aponta como benefícios do uso integrado do PEP "o ganho de tempo no preenchimento, a diminuição do viés de memória/esquecimentos, a completitude das informações e o seu potencial para uso em pesquisas científicas". Porém, pondera que a questão da privacidade de dados de pacientes, dados sigilosos por natureza, é um grande desafio frente ao risco de obtenção, uso e divulgação indevidos de tais dados. E, ainda, explica que "a realidade é que certamente aparecerão escândalos de vazamento de dados sigilosos, seja por descuido de alguns cientistas ou por invasões propositais", mencionando que a solução para tais enfrentamentos passa pela "conscientização dos cientistas sobre a importância da privacidade e o desenvolvimento de protocolos de segurança cada vez mais rígidos", a exemplo da criptografia (CHIAVEGATTO FILHO, 2015, p. 331).

Martorell *et al.* (2016) realizaram um trabalho de pesquisa que teve como objetivo estudar a exposição de pacientes, promovida por médicos e dentistas, na rede social Facebook. Os dados foram coletados entre os meses de agosto e setembro de 2013, por meio da seleção retrospectiva de 39 imagens publicadas por 17 profissionais. Nestas imagens, era possível identificar situações de quebra de sigilo e/ou privacidade por parte dos profissionais.

A escolha do Facebook é justificada por Martorell *et al.* (2016, p. 325), visto que a rede social é a mais popular entre os brasileiros. As informações avaliadas no referido estudo foram obtidas a partir do acesso a imagens extraídas de "álbuns" de usuários. Para isso, a amostra incluiu os perfis de médicos ou cirurgiões-dentistas que são próximos dos autores do estudo ou têm amigos em comum com eles na referida rede social. Assim, relatam os autores que Martorell *et al.* (2016, p. 326):

> Essas imagens já haviam sido publicadas e foram armazenadas nos "álbuns" de 17 diferentes profissionais de saúde, dos quais 12 eram cirurgiões-dentistas e 5 eram médicos. No total, 39 imagens foram acessadas: 27 publicadas por cirurgiões-dentistas e 12 por médicos. Até a data final para a coleta de dados, as 39 imagens receberam um total de 310 comentários e 800 "curtidas".

Os dados obtidos são ainda mais específicos e alarmantes (MARTORELL *et al.*, 2016, p. 329-330):

- 11 imagens permitiram identificar diretamente as pessoas envolvidas, em 07 dentre tais imagens era possível identificar completamente os rostos das pessoas. Dentre os rostos passíveis de identificação foram observadas 03 imagens com crianças em fotos individuais e em 01 imagem era possível identificar o rosto de um grupo de 11 crianças;
- 15 imagens possibilitaram a visualização de partes de rostos de pessoas em centros cirúrgicos ou consultórios, com possibilidade de identificação relativa. Nas imagens publicadas pelos médicos, houve 01 imagem de um paciente escalpelado, possivelmente vítima de um acidente de trânsito. Nas imagens publicadas pelos cirurgiões-dentistas, eram frequentes as tomadas fotográficas de sorrisos, em alguns casos incluindo imagens "antes e depois", referentes às intervenções odontológicas realizadas pelos profissionais usuários da rede social;
- 11 imagens apresentavam outras partes específicas dos pacientes expostas, como dentes, placas gordurosas e mãos e braços sendo puncionados. Dentre as imagens publicadas pelos médicos, destacou-se 01 imagem que mostrava uma lesão causada pelo corte lacerativo do pescoço e nuca e um procedimento de aneurismectomia na artéria braquial, o que permitia a identificação de uma extensa cirurgia no braço do paciente.

Martorell *et al.* (2016, p.332) enfatizam que tal tipo de exposição tem consequências negativas para pacientes, profissionais de saúde e à sociedade, além de infringir diretamente os direitos humanos universais cuja consolidação vem sendo buscada ao longo de décadas. E, também, é necessário compreender de maneira mais aprofundada as razões pelas quais alguns profissionais da área da saúde assumem comportamento antiético, expondo indevidamente seus pacientes nas redes sociais. Alertam ainda que os "conselhos profissionais que supervisionam diferentes profissões de saúde precisam estar cientes da conduta virtual de seus membros inscritos e precisam desenvolver atividades contínuas tanto para orientação quanto para investigação de possíveis transgressões éticas". Além disso, importa ressaltar o papel importante das universidades na formação dos profissionais, utilizando-se, por exemplo, da Bioética e priorizando discussões interdisciplinares transversais ao longo da formação acadêmica.

4. OS DADOS PESSOAIS SENSÍVEIS SOB O OLHAR DA A LGPD E DE OUTRAS LEIS BRASILEIRAS

DONEDA (2012, p.11) antecipou as preocupações com a proteção de dados pessoais em redes sociais, de modo a concluir a existência de um equilíbrio um tanto difícil:

> O cerne do problema reside, portanto, justamente em se conciliar os imperativos inafastáveis deste modelo de negócios com as diversas normativas de proteção de dados que abordam justamente as modalidades de tratamento de dados, bem como com as legítimas expectativas dos seus próprios usuários de divulgação de informações pessoais.

Chega-se, portanto, ao ponto em que Direito e Informática precisam andar de mãos dadas, uma vez que se vive o paradigma *everyware*[8] (GREENFIELD, 2006, p. 09) que norteia o desenvolvimento de um meio ambiente digital que congrega ubiquidade, pervasividade e inteligência, sendo o elemento de ligação formado pelo conjunto de dados veiculados, capturados, tratados e armazenados. Na visão de Schwab (2016) vive-se a "Quarta Revolução Industrial", uma vez que três razões sustentam tal revolução: velocidade, amplitude e profundidade e, por último, impacto sistêmico. O autor explica que as mudanças estão ocorrendo em um ritmo exponencial e não linear, como tradicionalmente se busca descrever e entender a tecnologia. Além disso, a combinação de várias tecnologias (multiplataformas, multitarefas, entre outros) e a transformação de sistemas inteiros (desde países até empresas) "não está modificando apenas o 'o que' e o 'como' fazemos as coisas, mas também 'quem' somos" (SCHWAB, 2016, p. 13).

É neste contexto de transformação que os dados sensíveis e seu respectivo tratamento passam a assumir vital importância desde a esfera governamental até o usuário final da Internet. A Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709, de 14 de agosto de 2018, diferencia dados pessoais de dados pessoais sensíveis (art. 5º, incisos I e II), de maneira a deixar claro que todo tipo de dados que possa gerar discriminação, segregação ou outra forma de violência contra a pessoa, também estará sob a égide da legislação, inclusive dados referentes à saúde ou à vida sexual, bem como dados genéticos (BRASIL, 2018). Nesse

[8] Texto original: *"Ever more pervasive, ever harder to perceive, computing has leapt off desktop and insinuated itself into everyday life. Such ubiquitous information technology – ´everyware´ - will appear in many different contexts and take a wide variety of forms, but it will affect almost every one of us, whether we're aware of it or not"*. Tradução livre: "Cada vez mais difundida, cada vez mais difícil de perceber, a computação saltou da área de trabalho e se insinuou na vida cotidiana. Essa tecnologia da informação ubíqua – '*everyware*' - aparecerá em muitos contextos diferentes e assumirá uma grande variedade de formas, mas afetará quase todos nós, quer estejamos conscientes disso ou não.

sentido, a lei é abrangente e necessária frente às técnicas de tratamento de dados e aos abusos cometidos, a exemplo da exposição de dados de pacientes em redes sociais.

Em relação ao tratamento de dados, a LGPD define no art. 5º, inciso X, que (BRASIL, 2018):

> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Inclui, ainda, a anonimização, o bloqueio, a eliminação, a transferência internacional e o compartilhamento de dados (art. 5º, incisos XI a XVI) da LGPD (BRASIL, 2018). Desse modo, a lei não somente apresenta o que se entende por tratamento de dados, mas também esclarece as operações informatizadas ou não que tornam a definição abrangente e atualizada em qualquer tempo.

Além disso, no art. 3º, explicita que o tratamento tanto se refere às operações realizadas em território nacional (inciso I) quanto aos dados pessoais que tenham sido coletados em território nacional (inciso III), uma vez que o titular dos dados se encontre em território nacional no momento da coleta (art. 3º, § 1º) (BRASIL, 2018).

O tratamento de dados sensíveis foi merecedor de artigo específico (art. 11) na LGPD, frente à sua importância e preocupação com a tutela dessa categoria de dados pessoais. Tal artigo especifica em que hipóteses o tratamento de dados sensíveis poderá ocorrer, a saber:

> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Verifica-se, assim, hipóteses consideradas na LGPD são significativas e consistentes para abranger diversas situações fáticas, relacionando dados sensíveis e tratamento de dados.

Ressalta-se que a LGPD recepciona o consentimento como um dos elementos de tutela dos dados pessoais (art. 7º, inciso I e art. 8º) (BRASIL, 2018). De acordo com Doneda (2006, p. 375), a "[…] reflexão sobre o papel do consentimento para o tratamento de dados pessoais é necessária para retirá-lo de uma posição na qual, escorado na tecnicidade, ele poderia neutralizar a atuação dos direitos fundamentais". Assim,

> […] O consentimento para o tratamento dos dados pessoais toca diretamente elementos da própria personalidade, porém não dispõe destes elementos. Ele assume mais propriamente as vestes de um ato unilateral, cujo efeito é o de autorizar um determinado tratamento para os dados pessoais (DONEDA, 2006, p. 377-378).

Bioni (2019, p. 136) afirma que o consentimento permanece, ao longo das gerações[9] de leis de proteção de dados, como o "elemento nuclear da estratégia regulatória da privacidade informacional", de modo a "... apostar no indivíduo como um ser capaz, racional e hábil para controlar as suas informações pessoais". O autor então pondera que há que se balancear soluções que, "... por um lado, empoderem o titular dos dados pessoais, e, por outro lado, não deixem apenas sobre seus ombros a proteção de suas informações pessoais" (BIONI, 2019, p. 137).

Sob a ótica dos dados sensíveis de pacientes, cabe destacar o papel da autodeterminação informativa (art. 2º, inciso II), figurando como fundamento de proteção aos dados pessoais e ao respeito à privacidade (BRASIL, 2018). A autodeterminação informativa, de acordo com a definição dada pela Constituição Federal Alemã, é um direito de personalidade, que garante ao indivíduo o direito de controlar a emissão e utilização de seus dados pessoais (ALEMANHA, 1983). Por isso, a autodeterminação informativa está tão ligada à privacidade, retomando-se a definição dada por Westin (1968, p. 7), a saber: "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others*"[10]. Assim, a autodeterminação informativa de cada indivíduo é assegurada pelo conceito de titularidade sobre seus dados pessoais.

Ponto relevante e estritamente ligado aos dados sensíveis de pacientes é a discriminação, sendo que a LGPD em seu art. 6º, inciso IX, explicita que as atividades de tratamento de dados pessoais deverão observar a boa-fé e o princípio da não discriminação,

[9] O autor aponta que existem quatro gerações de leis de proteção de dados pessoais. Ver: BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2ª. ed. Rio de Janeiro: Forense, 2019. p. 114-117.

[10] Tradução livre: "A reivindicação de indivíduos, grupos ou instituições de determinar por si mesmos quando, como e até que ponto as informações sobre eles são comunicadas aos outros".

visando não permitir o uso e tratamento de dados para fins discriminatórios ilícitos ou abusivos.

A discriminação pode resultar do tratamento de dados, sendo considerada um efeito colateral perigoso, visto que ao se determinar quais indivíduos compõem um perfil, por exemplo, pode-se gerar discriminação pela não oferta de determinado produto para um grupo de consumidores ou pela não oferta de uma vaga de trabalho para um certo grupo com determinada opção sexual ou religiosa.

Um exemplo relacionado à área da saúde que pode resultar em discriminação é a disposição de apresentar uma determinada doença. O Google possui uma *web page* denominada *Google Flu Trends* (GOOGLE, 2017), a qual foi especialmente criada para mostrar aos usuários quais são os locais em que a gripe e a dengue estão mais presentes, a partir das consultas realizada no buscador Google sobre estas doenças. O interesse do Google é estudar e permitir que pesquisas acadêmicas sejam realizadas a partir dos dados fornecidos no referido *site*. Porém, outros usos podem resultar da mesma base de dados.

A Constituição Federal de 1988 (BRASIL, 1988) preconiza no art. 5º que "todos são iguais perante lei, sem distinção de qualquer natureza". Seguindo o princípio constitucional, a Lei nº 7.716, de 05 de janeiro de 1989 define os crimes resultantes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional (BRASIL, 1989). Essa mesma lei pune com maior rigor a prática, induzimento ou incitação, pelos meios de comunicação social ou por publicação de qualquer natureza, da discriminação ou do preconceito de raça, por religião, etnia ou procedência nacional (art. 20, § 2º), sendo possível ao juiz determinar, dentre outras medidas, a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores (art. 20, § 3º, inciso III).

A LGPD não menciona especificamente nenhuma técnica ou mecanismo informático de tratamento de dados, mas prevê decisões destinadas a definir o perfil do titular dos dados, as quais estão relacionadas com o perfilhamento ou caracterização de perfil (*profiling*), de acordo com o art. 20, que estabelece (BRASIL, 2019):

> art. 20º - O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
>
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observando os segredos comercial e industrial.

De modo que o *profiling* está indiretamente considerado nas etapas de coleta, classificação, processamento, avaliação ou controle da informação; perfazendo-se assim o caminho que permite desde a exposição de dados sensíveis de pacientes em redes sociais até o resultado negativo desta exposição por meio da discriminação das pessoas nos mais variados ambientes que elas estejam e não somente no meio digital.

Finalmente, tem-se na LGPD um marco legal para tutelar o tratamento de dados pessoais inclusive no meio digital, de maneira a se frear os abusos e ilicitudes advindos da aplicação de técnicas informáticas sem a devida reflexão sobre as consequências na vida das pessoas. Afinal, se digitalmente as pessoas são um conjunto de "zeros" e "uns", na vida são indivíduos com nome, interesses e particularidades em esferas sobre as quais somente cada um deles pode decidir o que deseja ou não expor.

5. CONSIDERAÇÕES FINAIS

Devido à sua dinâmica, as redes sociais por vezes funcionam como espaços de compartilhamento de informação, conhecimento e experiência. Nesse contexto, a informação caminha ao lado da exposição, em que se observa a vulnerabilidade das pessoas em relação ao que é postado, veiculado e compartilhado na Internet, muitas vezes esquecendo-se de questões tão essenciais como a privacidade e a intimidade.

Especificamente em relação a dados sensíveis, importa ressaltar o uso de imagens de pacientes e de seus problemas de saúde, nas redes sociais. Observa-se que nem sempre os profissionais da área da saúde ou as empresas de Tecnologia da Informação e Comunicação (TIC), ao pretenderem expor ou coletar e tratar dados, mostram-se atentos às graves consequências decorrentes do uso de dados sensíveis de pacientes em redes sociais e que isso merece extrema cautela.

Na esteira constitucional de proteção à pessoa humana, sua dignidade, privacidade e intimidade, a Lei Geral de Proteção de Dados (LGPD) mostra algumas diretrizes, dentre as quais se destacam a autodeterminação informativa e a anonimização.

Além disso, vale salientar a necessária supervisão dos conselhos profissionais de saúde sobre a conduta digital de seus membros inscritos, bem como a orientação e investigação de eventuais transgressões éticas no uso de dados sensíveis de pacientes. Também é importante o papel das universidades na formação dos profissionais, mediante estudos interdisciplinares do tema. Enfim, buscar impedir ou, ao menos, mitigar os abusos e violações de direitos, decorrentes da aplicação de técnicas informáticas sem o cuidado e o respeito devido às pessoas.

REFERÊNCIAS

ALEMANHA. German Federal Constitutional Court**. BVerfG, 15 December 1983**. 1983. Disponível em: <http://www.servat.unibe.ch/dfr/bv065001.html#Rn003>. Acesso em: 15 abr. 2019.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. vol. 2, São Paulo: Saraiva, 1989.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2ª. ed. Rio de Janeiro: Forense, 2019.

BRASIL. **Constituição da República Federativa do Brasil**, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 15 abr. 2019.

_____. **Lei Nº 7.716 de 5 de janeiro de 1989.** 1989. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>. Acesso em: 15 abr. 2019.

_____. **Lei nº 10.406**, de 10 de janeiro de 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 15 abr. 2019.

_____. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 15 abr. 2019.

CAIRES, Bianca Rodrigues *et al.* Knowledge of healthcare professionals about rights of patient's images. **Einstein (São Paulo)**, vol. 13, no.2, São Paulo, apr./June, 2015. p.255-259.

CAPRA, Fritjof. **As conexões ocultas**: ciência para uma vida sustentável. São Paulo: Cultrix, 2002.

CARVALHAL, Gustavo Franco. Recomendações para a proteção da privacidade do paciente. **Revista Bioética** (Impr.), Vol. 25, no. 1, 2017. p. 39-43.

CAVALCANTI, Rafael. **Infográfico**: comportamento dos usuários brasileiros nas redes sociais. Nuvem Blog, 2013. Disponível em: <http://www.nuvemlab.com.br/blog/infografico-comportamento-dos-usuarios-brasileiros-nas-redes-sociais>. Acesso em: 15 abr. 2019.

CHIAVEGATTO FILHO, Alexandre Dias Porto. Uso de big data em saúde no Brasil: perspectivas para um futuro próximo. **Epidemiol. Serv. Saúde [online].** vol.24, no.2, 2015. p.325-332.

DAL BELLO, Cíntia. Visibilidade, vigilância, identidade e indexação: a questão da privacidade nas redes sociais digitais. **LOGOS 34**, O Estatuto da Cibercultura no Brasil. Vol.34, nº 01, 1º semestre 2011. Disponível em: <http://www.logos.uerj.br/PDFS/34/11_logos34_dalbello_visibilidade.pdf>. Acesso em: 15 abr. 2019.

DI FIORE, Bruno Henrique. **Teoria dos círculos concêntricos da vida privada e suas repercussões na praxe jurídica**. 2012. Disponível em: <www.flaviotartuce.adv.br>. Acesso em: 16 de abr. de 2014.

DONEDA, Danilo. Reflexões sobre proteção de dados pessoais em redes sociais. **Revista Internacional de Protección de Datos Personales**, Universidad de los Andes. Facultad de Derecho, Bogotá, Colombia, No. 1, julio-diciembre, 2012. p. 1-12.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FREITAS, Cinthia Obladen de Almendra. **A vulnerabilidade do consumidor e a exposição pública na internet**. In: Aires José Rover, Fernando Galindo. (Org.). III Encontro de Internacionalização do CONPEDI / Universidad Complutense de Madrid. 1ed. Madrid: Ediciones Laborum, 2015, v. 9, p. 76-101.

GOOGLE. **Google Flu Trendes and Google Dengue Trends**. 2017. Disponível em: <https://www.google.org/flutrends/about/>. Acesso em: 15 abr. 2019.

GREENFIELD, Adam. **Everyware**: The dawning age of ubiquitous computing. AIGA: New Riders, 2006.

HUGHES, Eric. **A Cypherpunk's Manifesto**. 1993. Disponível em <https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto>. Acesso em: 15 abr. 2019.

JOHNSON, Bobbie. **Privacy no longer a social norm, says Facebook founder**. The Guardian, 11 de janeiro de 2010. Disponível em: <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy>. Acesso em: 15 abr. 2019.

LICCARDI, Ilaria; PATO, Joseph; WEITZNER, Daniel J. Improving User Choice Through Better Mobile Apps Transparency and Permissions Analysis. **Journal of Privacy and Confidentiality**, v. 5, n. 2, Article 1, 2013. p. 1-55.

MARTELETO, Regina Maria. Análise de redes sociais: aplicação nos estudos de transferência da informação. **Ciência da Informação**, Brasília, v. 30, n. 1, jan./abr. 2001, p. 71-81.

MARTORELL, Leandro Brambilla *et al.* Uso de big data em saúde no Brasil: perspectivas para um futuro próximo. **Epidemiol. Serv. Saúde**, Brasília, vol.24, n. 2, april/june, 2015. p.325-332.

NASCIMENTO, Aline Tiduco Hossaka Molette. **Direito à vida privada e à intimidade do portador do HIV e sua proteção no ambiente de trabalho**. Monografia. Universidade Federal do Paraná. Setor de Ciências Jurídicas. Curso de Graduação em Direito, Curitiba-PR, 2009.

RECUERO, Raquel. **Redes Sociais na Internet**: Considerações Iniciais. E Compós, Vol. 2, 2005, p. 1-23. Disponível em: <http://www.compos.org.br/seer/index.php/e-compos/article/view/28/29>. Acesso em: 15 abr. 2019.

SCHWAB, Klaus. **A quarta revolução industrial**. Trad. Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SZANIAWSKI, Elimar. **Direitos de Personalidade e sua tutela**. São Paulo: Editora Revista dos Tribunais, 2005.

WARREN Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, dez. 1890. Disponível em: <http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm> Acesso em: 15 abr. 2019.

WESTIN, Alan F.. **Privacy and Freedom**. Bodley Head, London. 1968.