LIMITES À IMPLANTAÇÃO DE *CHIPS* SUBCUTÂNEOS: A TUTELA DA PRIVACIDADE COMO INSTRUMENTO DE PROTEÇÃO DA PESSOA NA SOCIEDADE DA INFORMAÇÃO

LIMITS TO THE IMPLANTATION OF SUBCUTANEOUS CHIP: THE PROTECTION OF PRIVACITY AS AN INSTRUMENT OF THE PROTECTION OF THE PERSON IN THE INFORMATION SOCIETY

Liliane Gonçalves Matos
Joyceane Bezerra de Menezes
Hian Silva Colaço

RESUMO

No contexto da sociedade de consumo, qualificada como informacional, exsurge a preocupação com os riscos da implantação de microchips em seres humanos, especialmente, quanto à privacidade dos envolvidos. Por meio de estudo analítico-descritivo, delinearam-se os novos contornos do direito à privacidade, redimensionando o tradicional conceito e ampliando a esfera privada. Como resultado, identificou-se que, embora haja sensação de segurança, o *chip* pode ensejar distorções e violações à privacidade. Conclui-se que o controle de dados sensíveis deve ser do seu titular, para vincular seu manuseio à finalidade que lhe foi autorizada, sob pena de se incindir na intensa vigilância e classificação.

Palavras-chaves: Microchips. Sociedade de informação. Direito de personalidade.

ABSTRACT

In the context of consumer society, qualified as informational, there is concern about the risks of microchips implantation in humans, especially regarding the privacy of those involved. Through an analytic-descriptive study, the new contours of the right to privacy were outlined, reshaping the traditional concept and expanding the private sphere. As a result, it has been identified that, while

there is a sense of security, the chip can lead to distortions and breaches of privacy. It is concluded that the control of sensitive data should be the responsibility of its owner, linking its handling to the purpose that was authorized, otherwise it is incindir in the intense surveillance and classification.

Keywords: Microchips. Information society. Right of personality.

INTRODUÇÃO

Com o avanço das tecnologias e ampliação dos meios de comunicação, o fluxo informacional ganhou velocidades insucetíveis de serem atingidas fora do ambiente virtual. A cada momento, os indivíduos renunciam parcela de sua privacidade e desnudam variados aspectos da sua vida na internet, em especial, nas redes sociais. Depositam informações pessoais nos mais variados sítios eletrônicos que oferecem serviços e produtos, ajudando a alimentar bancos de dados economicamente valiosos que, não raro, representam violações ao direito à privacidade. Nesse contexto, indaga-se se a privacidade seria um óbice ao pleno desenvolvimento dos "rearranjos virtuais"? Como definir a extensão e a proteção da privacidade no bojo de uma sociedade de consumo hiperconectada?

Compartilham-se indiscriminadamente dados sensíveis com empresas privadas sem se questionar sobre os riscos advindos do manuseio dessas informações. Renunciar à vida privada em troca de segurança ou com o desiderato de integrar-se a um determinado grupo social, não requer muito esforço dos usuários. Fato é que a circulação instantânea das informações associada às possibilidades de tratamento dos dados ajudou a operar mudanças significativas na delimitação da esfera privada e no conceito de privacidade o qual já não se confina à proteção do espaço geográfico do domicílio ou mesmo ao singular direito de estar só. Envolve também o direito ao autocontrole sobre as informações que correm sobre si e sobre o direito a não discriminação pelas escolhas pessoais.

No contexto da sociedade hiperconectada e, ao mesmo tempo, permeada pelo medo e pela insegurança, a comercialização de microchips subcutâneos exsurge com a proposta de oferecer, compilada e rapidamente, informações essenciais para um momento e para fins específicos.

Por meio do *chip*, armazenam-se dados pessoais para as mais diversas finalidades, sejam elas médicas, antissequestro, rastreadoras etc.

Diante disso, a tecnologia permite apresentar todo o histórico de saúde da pessoa pela simples leitura do chip. Dispensa-se que se colecione os exames, a cada consulta médica, e facilita o atendimento hospitalar, na medida em que o paciente informa o laudo de exames anteriores na própria pele. Nos casos de sequestro, pode-se informar às autoridades policiais a exata localização da vítima, facilitando o seu resgate em poucas horas, a fim de possibilitar a redução do tempo de trabalho da inteligência policial. O acesso de tantas informações pessoais, por vezes qualificadas em dados sensíveis, ampliará, entretanto, os riscos do manejo inadequado pela empresa, seja no desvio de finalidades seja no compartilhamento com outras que lhe sejam parceiras.

A partir dessa problemática, objetiva-se analisar os riscos que as informações contidas no biochip podem trazer à esfera da vida privada e, principalmente, estabelecer os limites de manipulação desses dados pela empresa a qual administra o serviço. É de suma importância delineadar bem as finalidades para as quais os dados foram coletados e compilados no chip, a fim de que a sua utilização Não transborde esses fins, sob pena de se caminhar da sociedade de informação para uma sociedade de vigilância sem espaço para a vida privada.

Para a análise do problema, o artigo se divide em três tópicos. O primeiro aponta as possibilidades de uso de microchips, informando as peculidaridades que circundam o seu uso; o segundo, trata da evolução do conceito de privacidade e de sua reorganização no novo modelo social cujas bases estão, cada vez mais, fincadas na divulgação de dados pessoais. Por último, delineiam-se os limites e as balizas jurídicas para o manuseio e tratamento das informações coletadas pelas empresas administradoras dos microchips.

O DESENVOLVIMENTO DA TECNOLOGIA RADIO FREQUENCY IDENTIFICATION – RFID E A PROBLEMÁTICA DA IMPLANTAÇÃO DOS MICROCHIPS SUBCUTÂNEOS

A tecnologia "radio frequency identification - RFID" surgiu, na década de 1980, como uma solução para os sistemas de rastreamento e controle de acesso[1]. Em 1999, o Massachusetts Institute of Technology (MIT), juntamente com outros centros de pesquisa, centraram-se no desenvolvimento de uma arquitetura que utilizasse os recursos das tecnologias baseadas em radiofrequência para servir de referência ao desenvolvimento de novas aplicações de rastreamento e localização de produtos. Desse estudo, adveio o Código Eletrônico de Produtos - EPC (Electronic Product Code). O EPC definiu a arquitetura de identificação de produtos que utilizava os recursos proporcionados pelos sinais de radiofrequência e foi chamada posteriormente de RFID (Radio Frequency Identification) ou Identificação por Radiofrequência.

Inicialmente vinculada ao rastreio de aeronaves, a utilidade do sistema de radiofrequência foi disseminada ao longo dos últimos anos[2]. A *antiga nova* tecnologia, está presente desde o cadastro biométrico do cartão magnético aos biochips, "não sendo exclusivo de um setor do mercado, mas fazendo parte de uma cadeia de negócios já que oferece nova visibilidade nas áreas de operação, nos parceiros de comercialização ou ajudando a identificar problemas" (STEFANELLO, 2013, p. 30).

Essa mesma tecnologia também é utilizada nas etiquetas inteligentes, haja vista que são etiquetas eletrônicas com microchip instaladas nos produtos. Esse chip, por meio de "ondas de radio frequência, a qual possui metal ou carbono como antena, promoverá o rastreamento" (SANTANA, 2005, s. p.). A partir do uso dessas etiquetas, o mercado passou a adotar a referida tecnologia em diversos setores. Como o caso do laboratório de Los Alamos, nos Estados Unidos, que, para rastrear materiais nucleares, idealizou um transponder identificador colocado em cada caminhão, informando a localização exata do motorista (GONZALEZ; HWANG; MONTEIRO, 2013, s. p.). Ou, no caso do sistema de biometria utilizado nos bancos, por meio do qual são reconhecidas as medidas físicas ou comportamentais exclusivas de um indivíduo (BANCO BRADESCO, s/d,

p. 01). No Bradesco S/A, o dispositivo age como *scanner* para capturar a imagem do padrão vascular da mão, autenticando-a toda vez que consumidor utilizar o autoatendimento.

Após o episódio de 11 de Setembro, os EUA almejaram, por meio do uso de chips de identificação, a possibilidade de colher informações pessoais dos viajantes, caso o chip estivesse instalado nos passaportes. Essa novidade foi recebida com muita preocupação entre defensores dos consumidores e da privacidade, em razão do alto potencial de espionagem e acesso a informações pessoais contidas nos chips (GONZALEZ; HWANG; MONTEIRO, 2013, s. p.).

No âmbito do sistema penal, os microchips são usados para "monitorar detentos". Acompanha-se uma nova forma de punição e de vigilância do condenado que desponta como uma das soluções possíveis para desafogar o sistema penitenciário castigado pela superlotação (CONTE, 2010, s.p.). Dentre as principais opções técnicas de monitoramento eletrônico de infratores, há a pulseira, a tornozeleira, o cinto e o microchip implantado no corpo humano, ficando a critério de cada Estado a escolha (BRANCO, 2010, s.p.).

No Japão, a principal função atribuída aos microchips é a de rastrear os alunos que eventualmente forem sequestrados. Para tanto, o chip tem sido instalado até em uniformes escolares (FOLHA DE SÃO PAULO, 2004, s.p.). Inspirado, na ideia japonesa, o município baiano de Vitória da Conquista, por iniciativa da Secretaria de Educação no Centro de Educação Paulo Freire (CAIC), implantou o chip no fardamento dos alunos da rede municipal de ensino. Como esse município recebeu a nota mais baixa do MEC em toda a rede municipal de ensino do país, visava-se, com o uso do dispositivo, monitorar a frequência e assiduidade escolar dos alunos (NASSIF, 2012, s.p.).

Na saúde, é importante lembrar "o case" do Hospital Jacob Medical Center, da cidade de Nova York, que já utiliza a tecnologia. O projeto piloto, cuja tecnologia é da Siemens, tem o objetivo de reduzir o tempo gasto em tarefas administrativas e aumentar a precisão dos registros médicos. As pulseiras, assim, armazenam dados como nome, sexo, data de nascimento e número do registro médico dos pacientes que serão acessados pelos médicos e enfermeiras, portando computadores de mão (PDAs)

integrados a leitores de RFID. O diretor executivo de clientes da Siemens Business Services, Jerry Moy, declarou que o paciente não pode escolher entre usar ou não as pulseiras com chips RFID, pois eles precisam ser identificados rapidamente pelos médicos. (KENDALL, 2005, s.p.)

Sob essa perspectiva, no caso de uma emergência, o chip pode ajudar a salvar vidas. Dispensa-se a necessidade de realização prévia de testes de grupo sanguíneo, alergias ou doenças crônicas, bem como a averiguação do histórico de exames e de medicamentos usados pelo paciente, facilitando, por conseguinte, o diagnóstico médico.

Diante da possibilidade de armazenamento de dados de identificação humana, importa definir o que se entende como chip. Em linhas gerais, pode-se dizer: a "RFID é uma tecnologia de identificação que utiliza a rádio frequência e não a luz, como no caso do sistema de código de barras, para capturar dados" (PINHEIRO, 2004, p. 01). Possui três elementos estruturais, quais sejam: *tags*[3]*, leitoras*[4] *e computadores*[5]*,* podendo ainda integrar outros componentes como antenas, sensores, atuadores, *middlewares* e *softwares*.

Diante dos avanços do uso do sistema RFID, o governo americano conferiu ao Dr. Carl Sanders[6], especialista da área de Engenharia Eletrônica e cientista a serviço do governo americano (MELO, 2014, p. 60), a tarefa de desenvolver o microchip que pudesse ser implantado sob a pele, por meio de uma agulha hipodérmica. Nesse passo, Carl Sander, auxiliado por uma equipe de engenheiros, passou a desenvolver o microchip para identificação de humanos e controle mundial com o propósito de comércio global (SANDERS, 2011, s. p.).

Portanto, o *biochip* é realidade. Desde 2003, já se noticiava, de acordo com o jornal "*La última generación*", os riscos que ele pode trazer, "*es cierto que este sistema puede ofrecer grandes alternativas para la tecnología y la humanidad, pero puede ser un arma de doble filo. Por esa razón es importante estar alertas, sobre que dispositivos quieren introducir en el ámbito tecnológico*". Essa tecnologia visa estabelecer a uma nova ordem mundial, como bem previa o filósofo Deleuze (1992, s. p.), baseada no controle das informações.

O chip se conserva dentro de uma cápsula que mede 7mm de comprimento e 0,75mm em largura, mais ou menos o tamanho de um grão

de arroz, podendo ser implantado sob a pele com uma seringa. Contém um *transponder* que consiste em um sistema de armazenamento e leitura de informação em ondas como controle remoto e uma bateria de lítio recarregável pelas mudanças da temperatura da pele, por um circuito termopar o qual produz uma corrente elétrica com flutuações da temperatura do corpo.

Trata-se, assim, de uma etiqueta eletrônica avançada, que utiliza a tecnologia de localização por satélite GPS, fazendo o rastreamento do usuário (REINALDO FILHO, 2006). Nesse entremente, o dispositivo emite um sinal de rádio, na frequência de 125 Kilohertz, além de conter um número de série único que pode ser lido por scanner e posteriormente usado para acessar o banco de dados contendo informações pessoais do usuário (CHIP, 2013, s. p.).

No que tange à extensão, verifica-se que existem dois tipos de chips subcutâneos: o RF Tag Passivo e o RF Tag Ativo. O RF tag passivo opera sem bateria, tem custo mais barato e vida útil ilimitada. Geralmente é do tipo só leitura, usado em curta distância (SANTANA, 2005, s. p.). Pode ser utilizado também para armazenar dados médicos, pois permite identificar pacientes cardíacos ou com Alzheimer, por exemplo, porém é necessário que o hospital disponha de estrutura tecnológica para ler os dados (REINALDO FILHO, 2006, s. p.).

O segundo tipo, objeto do presente estudo, é mais invasivo. O RF tag ativo é alimentado por bateria interna, possui custo mais alto e pode ser de escrita e leitura, ou seja, pode ser submetido à reescrita (SANTANA, 2005, s. p.). Esse tipo é utilizado para monitorar o movimento de pessoas, pois permite controlar a localização por satélite GPS e, assim, rastrear o usuário (REINALDO FILHO, 2006, s. p.).

A tecnologia foi tão bem recebida, que foi utilizada em vários países. Em Barcelona, na Espanha, o *chip* serve de controle de ingresso de pessoas em casas noturnas, tal como a *Baja Beach Club,* conforme dados obtidos pela revista *Isto É* (RAINHA MARIA, 2004, s. p.). Na Suécia, um edifício comercial em Estocolmo quer que os seus 700 (setecentos) funcionários instalem o chips subcultâneos para ter acesso às suas dependências (BBC, 2015, s. p.). Por exemplo, Elicio da Costa, condômino, a partir da implantação do *chip* de RFID na mão, abre a porta da frente, entra nas

salas do escritório e até aciona a máquina de fotocópia pela aproximação do *chip* ao leitor na parede. O objetivo é que, no futuro, o *chip* sirva para logar em computadores e realizar pagamentos com o mero toque da mão (BBC, 2015, s. p.).

Por sua vez, o Banco Nacional de Westminster, no Reino Unido, também se rendeu ao produto. Considerando-se as vantagens que se poderia ter com o uso de chips subcutâneos, lançou-se uma corrida para desenvolver um cartão de crédito que não precisasse de PIN ou senhas. O Banco trabalha na criação de um cartão onde possa ser instalado no corpo humano, o Mondexsmartcard (O ARQUIVO, 2013, s. p.).

Além das comodidades, a tecnologia oportuniza o monitoramento do acesso de empregados às áreas de segurança restritas. É o caso da empresa de vídeo vigilância *Citywatcher.com*, de Cincinnati, nos EUA, a primeira a utilizar os *chips* para essa finalidade. A Secretaria de Justiça do México, também, viu, no uso da tecnologia, como o imediato desígnico, a expectativa de controlar o fluxo de acesso a áreas que armazenam informações sigilosas sobre o narcotráfico (TERRA, 2006, s. p.).

A empresa norte-americana *Three Square Market*, que atua na área de tecnologia, por sua vez, substituiu os crachás, chaves e senhas de acesso aos computadores e aos demais equipamentos eletrônicos dos empregados pelos microchips[7]. A empresa que forneceu a tecnologia noticiou que o Brasil é o seu mercado em potencial[8]cujas demandas vão da seara penal, com a perspectiva de substituir as tornozeleiras eletrônicas, à médica, podendo, inclusive, funcionar como método contraceptivo[9][10].

No Brasil, em meados de 2006, veio à tona a primeira notícia de implante de chip de monitoramento sob a pele. Essa ideia parecia polêmica e assustadora, mas já havia 42 (quarenta e duas) famílias usando o chip subcutâneo e duas mil pessoas na fila de espera por uma oportunidade, conforme dados da RCI First Security and Intelligence Advising, empresa que monitora os implantes no Brasil (JANETH, 2006, s. p.). O rastreamento desses *chips* ocorre, nos EUA, onde está situada a base de monitoramento. De lá é possível rastrear pessoas em todo o mundo, ainda que a distância geográfica faça o custo desse rastreamento ser elevado.

É por isso que, buscando reduzir os custos do serviço, espera-se a instalação da base de monitoramento no Brasil (CHIP, 2013, s. p.). Nessa

trilha, antes que o implante do chip possa ser realizado, no país[11], é necessário que a FDA (Administração de Drogas e Alimentos dos Estados Unidos), órgão americano, regulamente o seu uso. Somente após isso, é que se pode protocolar o pedido de registro na Agência Nacional de Vigilância Sanitária (ANVISA). Até o presente momento, não houve qualquer pedido de regulamentação dessa tecnologia conforme dados obtidos pela Wnews (JANETH, 2006, s. p.).

Enquanto não se resolvem as questões burocráticas, os estudos avançam, à medida que se busca verificar qual o melhor local para aplicação do biochip no corpo humano. Dispendidos mais de 1,5 (um, cinco) milhões de dólares em estudos, identificaram apenas duas regiões do corpo como as mais apropriadas: a testa, debaixo do couro cabeludo, e a mão, especificamente a direita, pois o carregamento automático da pilha precisa de mudanças rápidas de temperatura sem falar das suas consequências sob a pele (SANDERS, 2011, s. p.).

É de bom alvitre mencionar que a implantação deve ser realizada por um médico[12]. Este, por meio de procedimento cirúrgico, instalará o chip sob a pele devendo o cliente pagar pelo ato e manutenção mensal. Para isso, o usuário deve preencher um formulário, no qual conterá suas informações pessoais e assinar o contrato de consentimento para fins de entendimento do fato. Este produzirá todos os efeitos do contrato de serviços (REINALDO FILHO, 2006, s. p.).

Assim, verifica-se que o microchip tem por finalidade armazenar informações sobre seu usuário, tais como: histórico de vida, judicial, profissional, saúde e dados financeiros; e, por meio de impulsos, envia um sinal numérico, fornecendo elementos de dados em intervalos regulares. Esses dados enviados consistem em informações essenciais para rastrear seu portador (SANDERS, 2011, s. p.).

A REENGENHARIA DA PRIVACIDADE NA SOCIEDADE DE VIGILÂNCIA

Diante dessas evidências, questionam-se os riscos decorrentes do manuseio de dados sensíveis, os quais representam os traços mais ín-

timos da personalidade dos usuários, pelas empresas administradoras dos microchips, cujo uso e compartilhamento indiscriminado revela alto potencial lesivo à privacidade.

A partir da colisão entre os direitos fundamentais da informação e da privacidade, exige-se do intérprete o sopesamento de interesses para minimizar os efeitos dos direitos em jogo. Assim, é de fundamental importância que se tenha bem delineado o conceito de direito de privacidade, para delimitar parâmetros à solução diante do possível conflito entre o espaço da esfera privada, como campo do direito de personalidade, e o direito a circular as informação, à luz dos princípios da unidade do ordenamento, da concordância prática e da proporcionalidade (FARIAS, 2000, p. 122).

Dessa forma, percebe-se que, diante de conflitos envolvendo interesses juridicamente relevantes no âmbito das relações virtuais, a "instância de controle valorativo dos atos privados deverá agir a fim de identificar o interesse merecedor de tutela preferencial em cada caso concreto", ou seja, se o direito à privacidade deverá ceder perante o direito à informação ou não (COLAÇO; RODRIGUES; 2017, p. 1139). Mas, qual seria o conceito moderno de privacidade a ser tutelado? Qual a origem e substrato da formulação desse direito?

Para Maria Celina Bodin de Moraes (2010, p. 85), o direito à privacidade, como um dos direitos da personalidade, representa o desdobramento do princípio jurídico da liberdade, o qual, junto aos princípios da solidariedade, da integridade psicofísica e da igualdade, compõe os corolários do valor axiológico da dignidade da pessoa humana. Rodrigues e Andrade (2016, p.99) sustentam que "o direito à privacidade é uma espécie de direitos fundamentais, cujo fundamento repousa no princípio da dignidade humana", consubstanciado como "o valor próprio que identifica o ser humano como tal" (SARLET, 2004, p. 38-39).

A ideia de privacidade surge, então, quando o desejo de intimidade assinalou o "fim das relações sociais recíprocas entre os estratos superiores e aqueles inferiores do regime feudal". Tal fato marcou o início do "novo alinhamento de classes que estava destinado a se refletir numa luta de classes sem tréguas e nas reivindicações individualistas de um período ulterior" (RODOTÀ, 2008, p. 26).

Nesse contexto, as primeiras formas de invocação ao direito à privacidade estão relacionadas ao processo de desintegração do regime feudal, quando os indivíduos não possuíam o direito de reservar-se ao silêncio ou de ficar só, pois a sociedade era organizada de modo que somente poucos senhores ou monges tinham acesso ao isolamento. Nesse contexto, com o declínio do sistema feudal e a ascensão da burguesia, o gozo do silêncio e do isolamento colocou-se como poder de expressivo valor econômico para a classe burguesa.

Com o passar dos tempos, e fazendo um corte histórico, importantes efeitos decorreram da eclosão das revoluções industriais. A brusca modificação no quadro social, no conceito de privacidade, a superação das fronteiras entre o espaço público e o espaço privado, bem como o desenvolvimentodo chamado "direito de estar só" marcaram a nova sociedade. O indivíduo buscava "proteção jurídica àqueles espaços livres de vigilância para o desenvolvimento da personalidade, a defesa de uma existência pessoal única contra perturbações exteriores, como o assédio e a observação" (KONDER, 2013, p. 357).

Essa dialética com a realidade externa, a partir das transformações dos modelos sociais, exigiu o redimensionamento do perfil desse direito, livrando-o das amarras estáticas de um direito subjetivo. Com a emersão do momento coletivo e do aspecto ligado ao controle do poder, abandona-se o discurso fechado em torno das fronteiras de uma determinada classe social, fazendo esse direito ganhar projeção sobre a coletividade, fato esse que modifica qualitativamente a forma de tutelá-lo.

Nessa linha, a evolução da noção de privacidade pode ser resumida a partir de quatro "paradoxos": "1) do direito a ser deixado só ao direito de manter controle sobre as informações que lhe digam respeito; 2) da privacidade ao direito à autodeterminação informativa; 3) da privacidade à não-discriminação e 4) do sigilo ao controle" (RODOTÀ, 2008, p. 97-98).

Assim, os novos desafios da privacidade transitam pela ampliação da tutela da esfera privada dos sujeitos cujas informações são coletadas e precisam exercer controle sobre estas. Conferiu-se função sociopolítica à privacidade, com o fito de proteger as informações atribuídas às opiniões políticas ou sindicais (consideradas como núcleo duro da privacidade),

de modo a impedir qualquer forma de controle público e estigmatização social decorrente da utilização dessas informações. Porém, a visão de privacidade associada à tutela da imagem, do sigilo profissional, de comunicações e bancário e à inviolabilidade de domicílio se mostrava ainda insuficiente para proteger a demanda social plural e multifacetada[13] na esfera de sua subjetividade.

Diante dessas tendências, percebe-se que a definição mais ampla de privacidade a tutelar às vissitudes da sociedade informacional implica no "direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" (RODOTÀ, 2008, p. 109).

Para Rodotà "vivemos num tempo em que as questões relacionadas à proteção de dados pessoais se caracterizam por uma abordagem marcadamente contraditória – de fato, uma verdadeira esquizofrenia social, política e institucional" (2008, p. 24). Desse modo, no ambiente em que a informação se tornou a arma mais eficaz e a "moeda de troca" mais valiosa que se tem na sociedade, o conceito de privacidade precisou acompanhar a modernização e se ampliar.

Todo o avanço científico e tecnológico que cunhou o novo modelo de sociedade trouxe consigo mais do que uma necessidade, um direito[14] de informar e de ser informado (TEPEDINO; TEIXEIRA; ALMEIDA, 2016, p. 254). Correlacionado à autodeterminação informativa, o direito à privacidade envolve até o chamado direito de não saber (RODOTÁ, 2008, p. 92). Nessa perspectiva, a internet ocupa o lugar de destaque na difusão das informações por ter capacidade de interligar, instantânea e simultaneamente, vários indivíduos em locais distintos. O contínuo fluxo de informações chega a despertar atenção sobre a progressiva tendência da redução da área destinada ao sigilo e da crescente liberação dos dados econômicos.

Em uma sociedade na qual os simples eventos do cotidiano são compartilhados imediatamente e as informações se propagam quase que na *velocidade da luz*, com crescente aceitação e exposição dos indivíduos na rede, a "privacidade passou a ser analisada no quadro de organização do poder, no qual a infraestrutura da informação é um dos seus componentes fundamentais" (RODOTÀ, 2008, p. 23 – 24). O direito

à privacidade encontra dificuldades em se sustentar como o "direito a ficar só"[15]na sociedade onde as barreiras geográficas foram minimizadas com a internet, o uso de tablets e smartphones pessoais e a interação por redes sociais e microblogs[16] (KONDER, 2013, p. 372).

Ademais, com todas as informações lançadas, é possível cruzar os dados e montar o perfil virtual dos indivíduos, o chamado "corpo eletrônico"[17] (RODOTÀ, 2007, p. 37). Tal fato ajuda na individualizaçãoda pessoa[18]eliminando as barreiras para que o mercado possa, a partir de então, tanto conhecer melhor seu público quanto direcionar seus esforços. Deve-se lembrar, porém, que não são todos os dados pessoais que interessarão à tutela constitucional. A rigor, a informação só é objeto de proteção, se relacionada à intimidade, à identidade e à autonomia (SAMPAIO, 1998,p. 369), são os chamados "dados sensíveis".[19]

O conjunto das informações as quais compõe o corpo eletrônico são igualmente merecedoras de tutela, todavia, deve-se conferir a categoria dos dados sensíveis[20] uma proteção reforçada, ao passo que a coleta e divulgação destes é suscetível de causar práticas discriminatórias e, portanto, violar, de modo mais intenso, os corolários do princípio jurídico da dignidade da pessoa humana.

Ao se "individuar tipos de informações, acerca das quais o cidadão estaria disposto a 'despir-se' completamente, no sentido de renunciar definitivamente a controlar as modalidades de seu tratamento e a atividade de sujeitos que as utilizam" (RODOTÀ, 2008, p. 36), legitima-se a violação aos direitos de personalidades dos titulares pelos atores econômicos. Ainda que se permita a utilização de alguns dados pelo mercado a fim de reduzir os custos de transação, não se pode escusar uma segura tutela ao núcleo duro da privacidade. Libera-se "o acesso às informações de caráter não pessoal, que constitui o objetivo primário das leis sobre a liberdade de informação"[21] (RODOTÀ, 2008, p. 72).

Esse novo rearranjo social, baseado na circulação contínua de dados, marca o desenvolvimento da sociedade cuja base é a informação. Nela o privado tende a ser definido sob o aspecto funcional. Neste ínterim, a esfera privada[22]se reorganiza, mais precisamente, com o "direito a manter o controle sobre as próprias informações"(RODOTÀ, 2008, p. 92). É a redefinição do conceito de privacidade sob as diretrizes do poder de controle[23].

Doneda (2010, p. 17) dispõe que as "informações pessoais assumem grande relevância, tanto como um bem jurídico como econômico", muitas vezes, transformando-se em uma "verdadeira *commodity* em torno da qual surgem novos modelos de negócio que, de uma forma ou de outra, procuram extrair valor monetário do intenso fluxo de informações pessoais proporcionado pelas modernas tecnologias da informação". Por esse motivo, a proteção dos dados pessoais continua sendo uma "utopia necessária[24]" para se garantir tanto a natureza democrática dos institutos políticos quanto que o indivíduo não seja coisificado.

Neste viés, o tratamento da personalidade arrisca ser submetido aos moldes negociais tipicamente patrimonialistas[25].As informações pessoais mais íntimas recorrentemente são comercializadas sob o manto da falaciosa liberdade formal, que nunca é suficiente nas relações desiguais (KONDER, 2010, p. 362). É nesse cenário que as garantias e os direitos fundamentais são, cada vez mais, desrespeitados.

A propagação desmedida dos dados e todas as suas implicações, para a esfera da privacidade, constituirá um fenômeno capaz de acirrar a era do medo, na qual imerge a sociedade de risco, qualificada por Ulrichs Beck (1992)[26]. A busca pela segurança se sobrepõe ao zelo pela privacidade e faz surgir o "homem de vidro"[27]nessa sociedade hipercomplexa. Assolado pelo medo, sentimento comum à humanidade na sociedade de riscos, o indivíduo se descortina.

A crescente sensação de ameaça se justifica na espera de um colapso iminente e nas mais diversas formas de violência que se manifestam no país. Tudo conduz ao delírio pelo uso de mecanismos de controle, monitoramento e vigilância[28]. Como descreve Bauman (2009, p. 63), "a arquitetura do medo e da intimidação espalha-se pelos espaços públicos das cidades, transformando-as sem cessar – embora furtivamente – em áreas extremamente vigiadas, dia e noite".

Na leitura de Konder (2013, p. 364) todos esses mecanismos de controle e vigilância implicam no comprometimento da privacidade e do corpo. Como se atribui a terceiros o poder de coletar e monitorar as informações sobre as pessoas, há o sacrifício da autodeterminação pela heterodeterminação.

De fato, o homem é centro de referência de informações. Dele sai ou nele ingressa uma série de dados que passam pelo processo de assimilação ou descarte (SAMPAIO,1998, p. 363). Nesse sentido, a partir do momento em que se contrata a empresa para implantar o microchip, deve-se preencher a ficha cadastral com as informações pessoais para que tais dispositivos possam reconhecê-las. Assim, os dados repassados para as empresas serão armazenados e cruzados a fim de mapear, e porque não dizer controlar, o indivíduo. Essa é a grande problemática associada ao uso do microchip que, tanto para uso médico quanto para fins de segurança, lida com dados pessoais.

Quando se trata do monitoramento de pessoas, o fato por si, já desperta maior preocupação, mormente quando houver o acesso aos dados sensíveis daqueles que, visando a sua maior segurança, renunciam parcela da sua privacidade. Com relação aos chips que armazenam dados de saúde, há o risco adicional de o vazamento das informações[29] gerar algum tipo de discriminação. Também não seria aceitável a cessão dos dados para empresas parceiras diferentes daquelas que figuravam no contrato inicial. Talvez isso pudesse resultar, por exemplo, na restrição da pessoa em contratar um plano de saúde ou um seguro de vida.

Pode-se criar, desse modo, perfis (RODRIGUES; ANDRADE, 2016, p. 95) dos pacientes, tanto para agrupá-los em possíveis usuários de remédios, como para discriminar àqueles que foram acometidos de certas doenças. O conjunto dessas informações constitui uma nova 'mercadoria' cujo comércio além de atingir a privacidade das pessoas pode modificar as relações entre fornecedores e consumidores de bens e serviços" (RODOTÀ, 2008, p. 62).

Assim, quando a pessoa portadora do chip passa por um local qualquer, equipado com sensores, sua identificação é checada automaticamente, e sua localização confirmada. Sensores nos mais diferentes lugares podem mapear as atividades dos implantados de modo a promover verdadeiro e completo sistema de vigilância. Um sistema interligado que pode ser utilizado pelas mais diversas instituições (policiais, militares, médicas, comerciais, industriais etc.), pelo simples cruzamento de dados de localização (FILHO, 2006).

Além de tudo isso, até o presente momento, só se tem notícia de duas empresas que administram os dados armazenados no microchip, ambas sediadas nos EUAs, fato este que pode complicar ou impossibilitar o controle de sua atuação.

PROTEÇÃO DE DADOS E UTILIZAÇÃO DE MICROCHIPS: CONEXÃO NECESSÁRIA

A era da 4ª Revolução Industrial, chamada também de Revolução Digital[30], guarda estrita relação com a difusão das informações. No ambiente digital tudo acontece com rapidez. Em frações de segundos, o recente acontecimento se torna notícia velha. A dinamicidade traz uma "nova angústia que nasce da consciência da forte defasagem entre a rapidez do progresso técnico-científico e a lentidão com que amadurece a capacidade de controle dos processos sociais que acompanham tal progresso" (RODOTÀ, 2008, p. 42).

As regras que disciplinam o direito à privacidade e ao sigilo de dados no Brasil, não tem, na maioria das vezes, o real alcance de todas as situações que podem envolvê-los, sendo necessária uma solução hermenêutica a qual evoque a unidade do ordenamento. Enquanto se procura solucionar o problema específico, outros já surgiram. Por vezes, aliás, há a sensação de que cresce a distância entre o veloz mundo da inovação tecnológica e aquele lentíssimo campo do planejamento sócio-político e jurídico.A resposta que o Judiciário ou o Legislativo podem/devem dar às situações concretas corre em descompasso com as novas necessidades da sociedade virtual. Tal fato desperta atenção para a necessidade de se preencher a defasagem com projetos de políticas públicas conscienciosas, elaborando remédios constitucionais eficientes (RODOTÀ, 2008, p. 42).

Para a atuação do Estado ser eficaz, faz-se jus observar as evoluções que mudaram profundamente o cenário que se apresenta. A difusão das possibilidades e das modalidades do tratamento das informações, principalmente. Há de se observar que "a sistematização de grandes volumes de informação tornou-se possível com o advento do processamento automatizado de informações, por meio de bancos de dados automatizados"

(DONEDA, 2010, p. 22) e, com a automação, surgiu uma série de novas possibilidades para a utilização de dados pessoais.

Para Rodrigues e Andrade (2016, p. 98) "o acesso a diversos produtos e serviços disponibilizados online não é concedido pela simples troca de determinada quantia. Na verdade, o modelo de negócio utilizado pela maior parte das plataformas digitais, como redes sociais, exige o pagamento pelo serviço com informações", que, na maioria das vezes, são dados pessoais dos usuários. São estes dados que despertam o maior interesse das empresas, pois com eles se conseguirá formar o perfil consumidor dos indivíduos.

É por esse motivo que, "seguindo os desenvolvimentos da tecnologia, percebe-se que a própria noção de 'arquivos de banco de dados' tende a se tornar insuficiente ou superada, e que a nova fronteira certamente não se encontra nos computadores pessoais", mas sim na noção de rede[31] (RODOTÀ, 2008, p. 44). "O valor de uma rede on-line é, então, condicionado à quantidade de informações pessoais que ela administra e à forma com que esses dados são utilizados" (RODRIGUES; ANDRADE, 2016, p. 98).

É por meio da venda de informações, da arrecadação de dados obtidos por *cookies* e da formação de perfis de usuários, entre outros, que se auferirá o valor que à rede on-line[32] é devida. A monetização da informação ocorre na mesma proporção do enfraquecimento da proteção dos dados do indivíduo. Demonstra-se, portanto, o principal motivo de se estabelecer os limites à coleta e manuseio dos dados. De acordo com Gustavo Tepedino (2014, p. 95),

> [...] com o avanço e barateamento da tecnologia de informação, sofisticam-se os acessos e controles, o cruzamento e a circulação de dados, sendo urgente restabelecer mecanismos de tutela dos direitos fundamentais, especialmente no que tange aos dados sensíveis. [...] Há que se definir quando, onde, como e para que fins podem ser colhidas informações pessoais, impedindo-se seu tratamento como ativo comercial ou expressão do poder político do Estado. Os critérios para tal definição hão de convergir para a melhor tutela dos direitos fundamentais em jogo.

Atrelado a isso, cresce o campo de atuação da sociedade de vigilância que busca esvaziar a proteção de dados por meio da propagação do

medo. Tenta-se relativizar a privacidade com o fundamento na segurança. A propaganda do medo foi reascendida no pós-11 de Setembro, acompanhada por constantes ataques terroristas pelo mundo.

Entretanto, embora a ameaça do terrorismo não seja comum no imaginário brasileiro, não se pode negar que a violência urbana é um fantasma recorrente a alimentar as demandas por mais vigilância e menos privacidade. Enquanto os atentados terroristas são atos pontuais entre os países mais ricos, o Brasil sedia vinte e uma das cinquenta cidades mais violentas do mundo, conforme dados do Conselho Cidadão para a Segurança Pública e a Justiça Penal[33]. Nesse contexto, o *terrorismo* torna-se um fato do quotidiano.

Embora não se possa nem se deva desqualificar as notícias sobre o aumento da criminalidade nas principais cidades, é de se observar que o discurso comum amplia um segmento do mercado o qual compromete a privacidade pelo controle e pela vigilância.

O moderno conceito de privacidade, "*controlofinformationaboutoneself*" justifica-se no poder autônomo de controle e requer um alargamento da perspectiva institucional. Supera-se, dessa forma, a lógica puramente proprietária e promove-se a integração dos controles individuais aos coletivos. Apesar de haver no mercado uma tendência à auto-regulamentação, com o automatismo do mercado, é necessário atribuir valor orientador para o futuro, justamente para garantir a plena expansão da liberdade e da democracia. Não se trata apenas de tutelar direitos, mas de salvaguardar e aguçar sensibilidades sociais, de estimular capacidades de reação (RODOTÀ, 2008, p. 58).

Há também o uso dos microchips como localizador antissequestros aparecendo como tentativa de dar maior segurança ao usuário. Ter, à disposição, um produto capaz de conceder padrões elevados de segurança rapidamente se torna desejável pela sociedade. É assim que, como já mencionado, existem 42 famílias que implantaram os chips, e outras se encontram em cadastro reserva desejando o produto (JANETH, 2006, s. p.). Apesar das vantagens que acompanham o produto, devem-se delinear os limites ao manuseio dos dados que serão administrados pelas empresas, pois, no momento da assinatura do contrato, o cliente autoriza que seus dados sensíveis sejam manuseados. Da contratação,

ao consumidor não é dado maiores esclarecimento sobre o serviço ou o tratamento dos dados. Ajusta-se apenas com expectativa do monitoramente sem se atentar para possíveis lacunas contratuais que firam aspectos da personalidade.

Diante de tal situação, pairam dúvidas acerca do total cumprimento das cláusulas contratuais por partes das empresas. Aos contratantes pouco ou quase nenhum poder de controle existe para se exigir o cumprimento do dispositivos contratuais. No caso de repasse desautorizado de informações, a outra empresa mesmo aquelas, porventura, parceiras da contratada, quais alternativas restariam ao contratante frustrado? Caber-lhe-ia tão somente reparação de danos?[34]

Em virtude da grande procura pelo produto subcultâneo, o legislativo pátrio imiscuiu-se sobre tais questões. O Deputado Roberto de Lucena - PV/SP apresentou Projeto de Lei de nº 6489/2016, cujo objeto se restringia a "vedar a implantação, de quaisquer tipos de mecanismos ou equipamentos eletrônicos e congêneres em cidadãos brasileiros, e dá outras providências". Buscou-se tratar a situação como se a disseminação do biochip não fosse palpável, ou como se habitasse no campo do imaginário. Não se considerou que o interesse pelo dispositivo poderia partir do próprio cidadão, buscando segurança ou facilidade no controle de sua saúde.

Ademais, é de bom alvitre lembrar que a Lei nº 12.965, de 23 de abril de 2014, chamada de Lei do Marco Civil da Internet, dispõe sobre a proteção da vida privada, dos dados pessoais, da inviolabilidade da intimidade e da operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional. Dessa forma, disciplinam-se aspectos relativos à internet e não à implantação e ao manejo de dados por intermédio de chipsubcultaneo. Essa situação é específica e deve ser abordada em lei própria, sensível aos problemas que podem surgir, não se limitando apenas a proibir o uso como o PL nº 6489/2016 aborda.

É assim que, no âmbito da legislação internacional, dois diplomas funcionais são estabelecidos como referência[35]: a Convenção do Conselho da Europa e a Recomendação da OCED. Este, promulgado em, 23

de setembro de 1980, contém as diretrizes relativas à proteção da vida privada e à circulação transnacional dos dados de caráter pessoal. Ao passo que aquele, cuja promulgação se deu quatro meses depois, a saber em 28 de janeiro de 1981, tratou da proteção das pessoas em relação à coleta automática de dados de caráter pessoal. Da síntese dessas duas disciplinas jurídicas da proteção dos dados, pode-se extrair seis princípios norteadores.

O primeiro deles é o princípio da *correlação na coleta e no tratamento das informações*; o segundo é da *exatidão dos dados coletados*, acompanhado pela obrigação de sua atualização; o terceiro dispõe sobre a *finalidade da coleta dos dados*, que deve ser conhecida antes que ocorra a coleta, e se especifica na relação entre os dados colhidos e na finalidade perseguida (*princípio da pertinência*); na relação entre a finalidade da coleta e na utilização dos dados (*princípio da utilização não-abusiva*); na eliminação ou na transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*);

A quarta base principiológica cuida da *publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público. O quinto trata do *acesso individual*, com finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correlação daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente. Por fim, o sexto cuida da *segurança física e lógica da coletânea dos dados*.

Com essa base principiológica, é possível se verificar a evolução do pensamento normativo sobre o manejo de informações. Passa-se de uma enunciação negativa e passiva de proteção de dados para uma positiva e dinâmica. Muda-se também a técnica jurídica utilizada cuja atribuição não se encontra mais nas mãos do sujeito privado que deveria questionar seu direito no órgão *ad hoc*depois de sua violação. Agora é concedido ao privado um poder de controle direito e contínuo sobre os coletores de informações, independentemente da existência real de uma violação. Em suma, a técnica se desloca para o bom funcionamento das regras sobre a circulação das informações (RODOTÀ, 2008, p. 60).

PRINCÍPIO DA FINALIDADE COMO LIMITE AO MANUSEIO DAS INFORMAÇÕES OBTIDAS A PARTIR DA IMPLANTAÇÃO DOS CHIPS SUBCUTÂNEOS

A sociedade da informação se especifica, portanto, como "sociedade dos serviços" da qual resultam duas consequências: quanto mais sofisticados tecnologicamente são os serviços, mais o indivíduo e suas informações pessoais são confiadas ao manuseio do fornecedor, e, quanto mais se alarga a rede de serviços, maiores são as possibilidades de interconexões das informações coletadas.

Esse conjunto de informações lançadas na rede, em função do contrato entre o fornecedor de serviço e o indivíduo-consumidor, faz com que o corpo material ceda em importância ao corpo virtual (RODOTÀ, 2008, p. 125). Trata-se da *digital persona*[36], *avatar* ou *pessoa virtual*, ilustrada pela transcrição de Pierre Lévy(1998, p. 30):

> O meu corpo pessoal é a manifestação temporária de um enorme 'hipercorpo' híbrido, social e tecnobiológico. O corpo contemporâneo se assemelha a uma chama. Ele costuma ser minúsculo, isolado, separado, quase imóvel. Depois, ele chega a fugir de si mesmo, intensificado pelos esportes ou pelas drogas, passa através de um satélite, ergue ao céu um braço virtual bem alto [...].

Assim "a inexistência de legislação específica que trate do direito à proteção de dados pessoais não pode constituir óbice para que se perfectibilize a sua defesa", de forma que"caberia ao Poder Judiciário, diante do caso concreto, tutelar a pretensão daqueles que pretendam ver seus dados pessoais protegidos, quer seja na relação de particulares, quer seja na seara do direito público" (RUARO; RODRIGUEZ, 2010, p. 176).

É neste contexto que o princípio da finalidade destoa em relação aos demais. Ao construir ponte entre o princípio da "legitimidade da coleta da informação" e "circulação dos dados", institui-se uma modalidade específica de controle e limitação da possibilidade de seu manuseio, regulando-se as operações de *matching*[37]. Na síntese de Rodrigues e Andrade (2016, p. 104), "qualquer uso de informações pessoais deve obedecer à finalidade comunicada ao interessado antes de sua coleta,

além de que a transferência delas a terceiros torna-se proibida, sem que haja a devida autorização".

No caso da implantação de chips, não será permitida a manipulação das informações consideradas dados sensíveis e a sua divulgação será adstrita aos interesses da pessoa considerada. Essa é solução mais consentânea para a situação que "cada vez desperta mais preocupações, sobretudo diante da disseminação desses artefatos eletrônicos"(FILHO, 2006, p. 01).Ou seja, as empresas que comercializam os microchips devem manusear os dados estritamente no campo autorizado por seus consumidores, sob risco de descumprir as cláusulas contratuais e ensejar a reparação equivalente prática proporcional aos danos sofridos pelos usuários do serviço.

Além da vinculação ao princípio da finalidade e da necessária atuação do Estado, por meio do Legislativo e do Judiciário, deve-se estabelecer mecanismo de controles individuais e de ações coletivas. Essas estratégias dizem respeito à efetivação de condições para que o indivíduo manifeste o seu consentimento adequado e livre, sem qualquer manipulação do meio. Dessa forma, entre as estratégias da tutela da privacidade exercidas pelo indivíduo tem-se: o "direito de oposição" a determinadas formas de coleta e de circulação de dados pessoais; o "direito a não saber" que pode ser entendido como todas aquelas formas de *direct marketing* que consiste justamente na invasão da esfera privada de um indivíduo com informações que ele não deseja; o "direito ao esquecimento" prevendo-se que algumas categorias de informações devam ser destruídas, ou conservadas somente em forma agregada e anônima (RODOTÀ, 2008, p. 133).

É só diante desses mecanismos que se poderá proporcionar segurança aos consumidores em questões as quais envolvam a comercialização dos chips que trabalham com dados sensíveis. Afora desta vinculação ética, o que se há é o descumprimento de cláusulas contratuais e má-fé da contratada que não se atentou aos princípios regidos pelo direito de privacidade. Esse comportamento não só é indesejável como pode causar consequências desastrosas aos direitos de personalidade, tornando a pessoa um mero objeto sem que se observe sua individualidade própria.

CONCLUSÃO

Diante do exposto, conclui-se que o conceito de privacidade se expandiu em resposta aos avanços da tecnologia e contexto da sociedade de informação. Hoje, o conceito de privacidade compreende não apenas a proteção ao espaço geográfico do domicílio ou o "direito de estar só", todavia envolve o autocontrole sobre as informações pertinentes a si próprio, incluindo o direito de não saber.

É nesta perspectiva que surge a preocupação com o uso da tecnologia RFID, utilizada no corpo humano, por meio do implante subcutâneo de microchips visando o sistema de armazenamento e leitura de informação essenciais para fins médicos, antissequestro, rastreadoras, etc. A tecnologia congrega informações importantes, em sua grande maioria, consideradas dados sensíveis, razão pela qual as operações nesse segmento inspiram o devido cuidado jurídico.

Como apenas duas empresas operam a implantação e adminsitracao de informações por microchip no mundo, é temerário que possam assumir elevado controle sobre dados sensíveis das pessoas. Assim, o manejo desses dados devem-se submeter ao rigor dos princípios da *correlação na coleta e no tratamento das informações*, da *exatidão dos dados coletados*, da *finalidade da coleta,circulação dos dados*, da *publicidade*, do *acesso pessoal* e da *segurança física e lógica da coletânea dos dados.*

No Brasil, o Marco civil da internet não seria suficiente para disciplinar a proteção jurídica desses dados veiculados em microchip. Mas, a partir da unidade do sistema juríco, especialmente, em virtude do cotejo dos direitos fundamentais, é possível uma solução hermenêutica capaz de contemplar os princípios internacionais que visam a disciplina dos dados.

Deve haver, assim, correlação entre a finalidade das informações coletadas e o manuseio dos dados. Essa extrita vinculação é o ponto nevrálgico do problema que se apresenta. É certo que a tecnologia RFID usada nos microchips pode trazer inúmeras comodidades e benefícios ao rearranjo que a vida moderna traz. Entretanto, tais modernidades não podem estar ligadas ao desrespeito dos direitos fundamentais, em especial à privacidade. Para que se possa gozar de todas as benevolências

prometidas, faz-se jus que haja um devido controle do manuseio das informações, por parte dos indivíduos e do Estado.

O devido controle se dará tanto por intermédio de ações legislativas, judiciais e até mesmo particulares. Essas ações estabelecem condições para que o indivíduo manifeste o seu consentimento adequado e livre, como o "direito de oposição", o "direito a não saber", o "direito ao esquecimento", entre outras. Assim, a vinculação à finalidade afixará limites previamente autorizados não se permitindo que dados sensíveis sejam expostos na lógica do mercado. Neste ínterim, a tênue linha entre a sociedade de informações e de vigilância, cujo risco repousa na massificação, classificação e controle da sociedade, não será rompida.

NOTAS

1 Esse sistema de radar foi inventado pelo físico escocês Robert Alexander que permitia a notificação da aproximação de aviões, mesmo eles ainda estando distantes, facilitando a preparação das defesas contra-ataques inimigos. Desse modo, estava implantado o primeirosistema de identificação por rádiofrequência (CIRIACO, 2009, s. p.).

2 Poirier, C; Mccolum, D, (20006) afirma que a maioria das novas tecnologias, após descobertas, levam em torno de 30 anos para serem colocadas em prática, desta forma, o RFID é uma das mais antigas novas tecnologias, que vem sofrendo grandes incentivos, para um maior crescimento em sua utilização.

3 As *tags* são um dos componentes mais importantes da tecnologia RFID (SANTINI, 2008, s.p.), é através delas que os dados podem ser enviados, recebidos e transmitidos. As *tags* são divididas em 3 grupos, segundo o IBM (2013): a) *tags passivas* são aquelas que não possuem baterias. Retiram sua energia quando em contato com o leitor para o qual encaminha as informações codificadas na sua memória; b) *tags ativas* são aquelas equipadas por uma fonte de energia parcial ou completa, da qual retiram sua energia; por fim, as c) *tagssemi-passivas* são aquelas que possuem sensores de condição. Não apenas uma bateria, mas circuitos que leem e transmitem diagnósticos de volta para o seu sistema de sensores. Estas informações são alimentadas nos sistemas, por meio do soft de rede. (STEFANELLO, 2013, p. 32).

4 Segundo Santini (2008, s. p.) os leitores têm a função de comunicar-se com as tags RFID através de uma antena, repassando as informações e, em alguns casos, processando-as para outros sistemas. À cerca dos leitores Stefanello (2013, p. 36) classifica os leitores como sendo o sistema nervoso central do hardware de um sistema RFID Lahini.

5 Os computadores, por sua vez, é o centro que receberá e armazenará todas as informações coletadas pela antena, bem como promoverá a destinação adequada do seu manuseio e coleta dos dados.

6 Dr. Carl Sandertrabalhou com o FBI, CIA, entre outras grandes empresas, além de agências de governos de outros países, no desenvolvimento de tecnologias de espionagens de segurança. Também recebeu do presidente americano o prêmio por desígnio de excelência (SANDERS, 2011, s.p.).

7 De um total de oitenta funcionários, sessenta e um optaram, voluntariamente, pelo implante subcutâneo do chip.

8 'Brasil será nosso próximo mercado', diz CEO que implantou chips no corpo de funcionários nos EUA." Disponível em: <http://www.bbc.com/portuguese/internacional-41033209?ocid=socialflow_facebook>. Acesso em 27 de agosto de 2017.

[9] Ele libera diariamente uma pequena dose do hormônio contraceptivo levonorgestrel. A administração do remédio pode se estender por até 16 anos e é programada pela paciente ou seu médico através de controle remoto. Caso a mulher decida engravidar, o chip pode ser desativado (VEJA.COM, 2014, s. p.).

[10] Em 1960 o médico baiano Elsimar Coutinho já desenvolvia pesquisas clínicas com implantes subcutâneos de acetato.

[11] Especula-se que a Motorola é a empresa que está produzindo o microchip para a Mondex Smartcard, porém a empresa VerichipCorp assinou um contrato sigiloso de distribuição exclusiva no Brasil para a implantação de milhares de chips localizadores subcutâneos (ANTI..., 2013, s.p.).

[12] Manica e Nucci (2017, p. 09) ao escrever sobre o uso de microchips como forma contraceptivo diz que "a implantação e a retirada das cápsulas de silicone são procedimentos médicos que envolvem o domínio de um aparato técnico e, portanto, uma dinâmica específica entre equipe médica e paciente/usuária, no consultório/ clínica".

[13] Para Rodotà (2008, p. 28) a privacidade, portanto, não pode ser considerada como uma noção unificadora, como um conceito que exprime exigências uniformemente difundidas na coletividade.

[14] Art. 5º IV, XIV, IX e XXXIII da Constituição Federal do Brasil de 1988, Lei 12.527/2012, Declaração Universal dos Direitos Humanos de 1948, entre outros.

[15] Konder (2013, p. 372) questiona-se "como pensar pensar o 'direito a ficar só' e a proteção de uma esfera de isolamento em uma comunidade virtual cujos membros já estão a quilômetros de distância, mas cuja exposição pessoal é maior e mais frequente do que entre vizinhos de condomínio? A proteção da privacidade contra agressões alheias demanda reformulação quando não é mais possível demarcar com clareza a separação entre a "esfera interna" e as "interferências externas".

[16] Já fazia o alerta entre nós, em 1989, Tepedino (2008, pp. 561-563).

[17] MACLUHAN (1964, p. 88) descreveu corpo eletrônico como "nossos dados, estruturados de forma a significarem para determinado sujeito uma nossa representação virtual – ou um avatar –, podem ser examinados no julgamento de uma concessão de uma linha de crédito, de um plano de saúde, a obtenção de um emprego, a passagem livre pela alfândega de um país, além de tantas outras hipóteses".

[18] Correlacionam o nome, sobrenome, sexo, preferências, local de residência, entre outros.

[19] Personal data is the new oil of the Internet and the new currency of the digital world. No discurso proferido na mesa redonda sobre coleta de dados, direcionamento e perfilação. Bruxelas, 31 de março de 2009, a Comissária europeia do consumo, MeglenaKuneva, deixou claro que a monetarização dos dados pessoais foi uma tendência amplamente antecipada e que hoje é vital para uma parcela bastante representativa de novos serviços e produtos. Para ela "os dados pessoais são o novo óleo da Internet e a nova moeda do mundo digital.

[20] A Lei nº 12.414/2011, conhecida como Lei do Cadastro Positivo de Dados, inseriu, no ordenamento jurídico nacional, o conceito de dados sensíveis no §3º, Art. 3º como as informações "petinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas".

[21] Perceba que, quanto ao mercado, é facilmente aceita a "disseminação e manejo dos dados econômicos, tanto como forma de diminuir os custos de transação nas relações negociais como de controle por parte da coletividade e não apenas dos órgãos públicos especializados" (RODOTÀ, 2008, p. 34 – 35). O problema reside mesmo em torno dos intitulados dados sensíveis.

[22] FRIEDMAN (1990, p. 184) A esfera privada pode ser definida como aquele conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo. Em consequência, a privacidade pode ser identificada com "a tutela das escolhas de vida contra toda forma de controle público e de estigmatização social".

[23] Possibilita-seao sujeito conhecer, controlar, endereçar e interromper o fluxo das informações relacionadas a ele.

[24] StefànoRodotà (2008, p. 42) usa a expressão para descrever a nova angústia que nasce da consciência da forte defasagem entre a rapidez do progresso técnico-científico e a lentidão com que amadurece a capacidade de controle dos processos sociais que acompanham tal progresso. Defende que, com muita frequência, a rápida obsolência das soluções jurídicas se originam por se referir a um único e isolado dado técnico do problema. Conclui afirmando que as dificuldades

em especificar estes princípios não derivam somente do fato de que se trata de regular uma realidade em contínua transformação, mas nasce da necessidade de se levar em consideração uma multiplicidade de exigências, interesses, valores, frequentemente em conflito entre si. Uma verdadeira utopia necessária já que por vezes, tem-se a sensação de que cresce a distância entre o velocíssimo mundo da inovação tecnológica e aquele lentíssimo do planejamento sócio-institucional.

25 Com dados precisos sobre os consumidores é possível, por exemplo, organizar um planejamento de produtos e vendas mais eficientes, ou mesmo uma publicidade voltada às reais características dos consumidores, dentre diversas outras possibilidades(DONEDA, 2010, p. 9).

26 O argumento central do livro Risk Society (1992) é que a sociedade industrial, caracterizada pela produção e distribuição de bens, foi deslocada pela sociedade de risco, na qual a distribuição dos riscos não corresponde às diferenças sociais, econômicas e geográficas da típica primeira modernidade.

27 Sobre o tema, v. Bodin de Moraes (2010, pp. 33-54).

28 Para Stefano Rodotà (2008, p. 113) os riscos da sociedade da vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos, o que qualifica tais sociedades como autoritárias ou ditatoriais.

29 Em seus estudos sobre o uso de microchips como métodos contraceptivos Manica e Nucci (2017, p.101) relatam que a possibilidade de outras pessoas acessarem o dispositivo, provocando ou inibindo a liberação da substância sem o controle/ciência da usuária foi levantada como uma das inseguranças do método. Assim, as críticas abordaram a necessidade, bem como os limites, de uma codificação dos dados dos dispositivos móveis que devem controlar os microchips, problematizando a possibilidade de eles serem invadidos e manipulados por terceiros, em uma espécie de "hackeamento" ovariano (ovarianhacking), inclusive com eventuais objetivos vingativos (revengepregnancy). Esse desdobramento seria similar ao que se conhece como pornografia de vingança (revengeporn), isto é, a circulação de fotografias e vídeos íntimos por ex-parceiros sexuais pelainternet como uma forma de se vingar do final do relacionamento afetivo. A gravidez de vingança seria um recurso (mais) possível ao se obter, sem autorização ou conhecimento da usuária, o controle do dispositivo que acionaria (ou não) a liberação do hormônio contraceptivo.

30 Para Klaus Schwab (2016), em A Quarta Revolução Industrial: estamos a bordo de uma revolução tecnológica que transformará fundamentalmente a forma como vivemos, trabalhamos e nos relacionamos. Em sua escala, alcance e complexidade, a transformação será diferente de qualquer coisa que o ser humano tenha experimentado antes" A quarta revolução industrial não é definida por um conjunto de tecnologias emergentes em si mesmas, mas a transição em direção a novos sistemas que foram construídos sobre a infraestrutura da revolução digital (anterior)".

31 Entendida como local área network, workstation, redes sociais, entre outras.

32 Neste sentido, tem-se o facebook, o instagram, a twitter, o google, o yahoo, entre outros.

33 Disponível em: <http://www.seguridadjusticiaypaz.org.mx/biblioteca/prensa/category/6-prensa>. Acesso em 28 de mai. 2017.

34 Por serem questões volúveis e que rapidamente se modificam, o campo do tratamento dos dados sensíveis deve ter base principiológica que consiga acompanhar a versatilidade da reorganização informativa (RODOTÀ, 2008, p. 57). Assim, não se trata unicamente "de tutelar direitos, mas de salvaguardar e aguçar sensibilidades sociais, de estimular capacidades de reação. As armas institucionais, longe de serem reduzidas, devem ser ternazmente enriquecidas" (RODOTÀ, 2008, p. 58).

35 JOINET, Louis. Étude des príncipesdirecteursconcernants le recours à des fichiers de personnesinformatisés, Nations Unies: Conseil Économique et Social (Doc. E/CN. 4/Sub. 2/1983/18), 1983; P. Sieghart, Producers for the Resolution of Conflicts of Interest in Data Protection, in Council of Europe – Camera deiDeputati, Legislation, cit., pp. 195 ss.

36 The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual". Roger Clarke. "The digital persona and its application to data surveillance", in: The Information Society, 10, 2 (junho 1994) apud Richard Turkington; Anita Allen. Privacy law. Cases and materials. St. Paul: West Group, 1999, p. 313.

37 Elaborações de perfis através da combinação de dados.

REFERÊNCIAS

BBC NEWS Brasil.com.**Empresas implantam chips nos funcionários para interagir com sistemas**. Disponível em: <http://www.bbc.com/portuguese/videos_e_fotos/2015/02/150130_chip_subcutaneo_pai>. Acesso em: 02 maio 2017.

BANCO BRADESCO. **Senhas e dispositivos de segurança**. Disponível em: <http://www.bradesco.com.br/html/classic/como-usar/senhas-e-dispositivos-deseguranca. shtm> Acesso em: 22 abr. 2017.

BAUMAN, Zygmunt, 1925. **Confiança e medo na cidade**. Tradução Eliana Aguiar. Rio de Janeiro: Jorge Zahar. ed.,2009.

BBC NEWS Brasil.com. **EUA liberam implante de chip em humanos**. Publicado em: 15 ago. 2004.Disponível em: <http://www.bbc.co.uk/portuguese/reporterbbc/story/2004/10/041015_chipebc.shtml>. Acesso em: 18 abr. 2017.

BRANCO, Agatha. **Algemado à tecnologia**. Publicado em: 20 de jan. 2010. Disponível em: <http://infogps.uol.com.br/blog/tag/tornozeleira/>. Acesso em: 03 maio 2017.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia / Escola Nacional de Defesa do Consumidor; elaboração Danilo Doneda. – Brasília: SDE/DPDC, 2010. Disponível em:<http://www.vidaedinheiro.gov.br/docs/Caderno_ProtecaoDadosPessoais.pdf>. Acesso em: 23 maio 2017.

CHIP implantável vendido nos E.U.A. Disponível em:<http://www.fimdostempos.net/marcadabesta/chip-eua.html>. Acesso em: 12 abr. 2017a.

CHIP tenta evitar sequestro. Disponível em:<http://www.celebrandodeus.com/noticias/noticia_Chip.asp**>.** Acesso em: 13 mar. 2017b.

CIRIACO, Douglas. **Como funciona a RFID?**. Publicado em: 17 ago. 2009. Disponível em: <http://www.tecmundo.com.br/tendencias/2601-como-funciona-a-rfid-.htm> Acesso em:01 abr. 2017.

CLARKE, Roger. **The digital persona and its application to data surveillance**. In: The Information Society, 10, 2 (junho 1994) apud TURKINGTON, Richard; ALLEN, Anita. Privacy law. Cases and materials. St. Paul: West Group, 1999.

CONTE, ChristianyPegorari.**Execução penal e o direito penal do futuro: uma análise sobre o sistema de monitoramento eletrônico de presos**. Revista dos Tribunais, v. 894, p. 401 abr. 2010.

COLAÇO, Hian Silva; RODRIGUES, Francisco Luciano Lima. **Merecimento de tutela na sociedade da informação**: reedificando as fronteiras do direito civil. Revista Quaestio Iuris, Rio de Janeiro, v. 10, nº 2, pp. 1125-1145, 2017.

DELEUZE, Gilles. **Post-scriptum sobre as sociedades de controle**. **Conversações**: 1972-1990. Rio de Janeiro: Ed. 34, 1992, p. 219-226. Tradução de Peter PálPelbart.

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

FARIAS, Edilsom Pereira de. **Colisão de direitos**: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. 2a ed. Porto Alegre: Sérgio Antonio Fabris Editor, 2000.

FILHO, Demócrito Reinaldo. **A implantação de chips em seres humanos para uso médico e os riscos à privacidade**. Boletim Jurídico, Uberaba/MG, a. 4, no 189. Disponível em: <http://www.boletimjuridico.com.br/doutrina/texto.asp?id=1450>. Acesso em: 21 maio 2017.

FOLHA DE SÃO PAULO. **Estados Unidos liberam implante de chip em humanos**. Publicado em: 15 out. 2004. Disponível em: <www1.folha.uol.com.br/folha/bbc/ult272u36147.shtml>. Acessoem: 21 maio 2017.

FRIEDMAN, Milton. **Capitalism and freedom**. Chicago: University of Chicago, 1990.

GONZALEZ, Antônio Galiza Cerdeira; HWANG, André; MONTEIRO, José Guilherme Tavares. **Identificação por rádio frequência**. Jan. 2013. Disponível em:< http://www.gta.ufrj.br/grad/13_1/rfid/cap2_1.html>. Acesso em: 09 abr. 2017.

IBM. **Controlando o RFID. 2013.** Disponível em:<http://www.ibm.com/br/ibm/ideasfromibm/rfid/061207/index1.phtml>. Acesso em 28 maio 2017.

JANET, Lucya. **42 FAMÍLIAS no Brasil têm Chips no Corpo**. Publicado em: 25 abr. 2006. Disponível em: <http://somostodosum.ig.com.br/clube/artigos/autoconhecimento/42-familias-no-brasil-tem-chips-no-corpo-15333.html>. Acesso em: 21 maio 2017.

JOINET, Louis. Étudedes príncipes directeursconcernantslerecours à desfichiers de personnesinformatisés, NationsUnies: ConseilÉconomique et Social (Doc. E/CN. 4/Sub. 2/1983/18), 1983.

KENDALL, S. **Hospital identifica pacientes por chip**. Publicado em: 3 mar. 2005. Disponível em: <http://idgnow.uol.com.br/AdPortalv5/ComputacaoCorporativaInterna.aspx?GUID=9E757DA8-3190-49FE-B2F9-B712BEFEF611&ChannelID=2000006>. Acesso em: 05 maio 2017.

KONDER, Carlos Nelson. **Privacidade e corpo**: convergências possíveis. Pensar, Fortaleza, v. 18, n. 2, p. 354-400, mai./ago. 2013.

LÉVY, Pierre.**Qu'est-ce que levirtuel?**. Paris: La Découverte, 1998.

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

MACLUHAN, Marshall. **Os meios de comunicação como extensões dos homens**. Tradução de Décio Pignatari. São Paulo: Cultrix, 1964, p. 88.

MAÑAS, José LuisPiñar. **El derecho fundamental a laprotección de datospersonales** (LOPD).In:Protección de datos de carácter personalenIberoamérica. José LuisPiñarMañas (dir.). Valencia: TirantLoBlanch, 2005, pp. 19-36.

MANICA, Daniela; NUCCI, Marina. **Horizontes Antropológicos**. Porto Alegre, ano 23, n. 47, p. 93-129, jan./abr. 2017. Disponível em:<http://www.scielo.br/pdf/ha/v23n47/0104-7183-ha-23-47-0093.pdf>. Acesso em: 06 out. 2017.

MELO, Miliane de. **A implantação de chip em seres humanos como forma de rastreamento eletrônico**: um estudo acerca da viabilidade de sua utilização à luz do princípio da dignidade da pessoa humana. Unisul de Fato e de Direito:

revista jurídica da Universidade do Sul de Santa Catarina, [S.l.], v. 5, n. 9, p. p. 343, out. 2014. ISSN 2358-601X. Disponível em: <http://www.portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/article/view/2461/1752>. Acesso em: 27 maio 2017. doi:http://dx.doi.org/10.19177/ufd.v5e92014p. 343.

MORAES, Maria Celina Bodin de. **Ampliando os direitos da personalidade**: na medida da pessoa humana. Rio de Janeiro: Renovar, 2010.

NASSIF, Luis. **Escola implanta chips em uniformes para monitorar alunos.** Publicado em 29 dez. 2012. Disponível em: <http://jornalggn.com.br/blog/luisnassif/escola-implanta-chips-em-uniformespara-monitorar-alunos> Acesso em: 21maio 2017.

OARQUIVO**. MONDEX e o biochip**. Disponível em:< http://oarquivo.com.br/temas-polemicos/religiao-cultos-e-outros/591-mondex-e-o-bichip.html>. Acesso em: 21 maio 2017.

PINHEIRO, José Mauricio Santos. **Rfid**: identificação por radiofrequência. Disponível em:<http://www.projetoderedes.com.br/artigos/artigo_identificacao_por_radiofrequencia.php>. Acessoem: 21 maio 2017.

POIRIER, C.; MCCOLUM, D. **Rfid**: StrateficImplemantation and ROI. J. Ross Publishing. [S.l.]: [s.n.], 2006.

RAINHA MARIA**. A NOVA era e a nova ordem mundial**. Publicado em:16 jun. 2004. Disponível em: <http://www.rainhamaria.com.br/Pagina/530/Implante-de-chip-torna-se-obrigatorio-emfrequentadores-de-casa-noturna-na-Espanha> Acesso em: 10 maio 2017.

REINALDO FILHO, Demócrito. **A implantação de chips em seres humanos para uso médico e os riscos à privacidade**. Jus Navigandi, Teresina, ano 11, n. 1191, 5 out. 2006. Disponível em: <http://jus.com.br/revista/texto/8721>. Acesso em: 21maio 2017.

RIO DE JANEIRO (Estado). Tribunal de Justiça. 8a Câmara Cível. **Apelação Civel. 1993.001.06617**. Relator Desembargador Geraldo Batista, v.u. Julgamento. 18 mar. 1997. Ementário: 07/1997 - n. 36 – 15/05/1997. Revista Direito do T.J.E.R.J., v. 33, p. 189, 1997.

RODRIGUES, Francisco Luciano Lima; ANDRADE, Luana Silveira de.**Direito à privacidade na sociedade da informação**: autodeterminação informacional como preservação da pessoa frente ao mercado. In:(Org.): MENEZES, Joyceane Bezerra de; RODRIGUES, Francisco Luciano Lima.**Pessoa e mercado sob a metodologia do direito civil-constitucional** [recurso eletrônico]. Santa Cruz do Sul: Esserenel Mondo, 2016, e-book.

RODOTÀ, Stefano. **A vida na sociedade de vigilância – a privacidade hoje**. Coord. Maria Celina Bondin de Morais. Tradução Danilo Doneda e Luciano Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. **O direito à proteção de dados pessoais na sociedade da informação**. Direito, Estado e Sociedade, Rio de Janeiro, v. 36, p. 178-199, jan./ jun. 2010.

SAMPAIO, Adércio Leite José. **Direito à intimidade e à vida privada**: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

SANDERS, Carl. **Criador do microchip para identificar humanos**. Publicado em: 17 set. 2011.Disponível em: <http://jesusverdadequeliberta-c.webnode.pt/news/carl-sanders-criador-domicrochip-para-identificar-humanos/>. Acesso em: 09 abr. 2017.

SANTANA, Sandra Regina Matias. **RFID:** Identificação por rádio frequência. São Paulo: FATEC - Faculdade de Tecnologia da Baixada Santista: 2005. Disponível em: <http://www.wirelessbrasil.org/wirelessbr/colaboradores/sandra_santana/rfid_01.html>. Acesso em: 15 abr. 2017.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. Porto Alegre: Livraria do Advogado, 2004.

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

STEFANELLO, André Luiz. **A utilização de RFID na identificação de pessoas**. Rio Grande do Sul: Universidade Federal de Santa Maria: 2013. Disponível em:< http://repositorio.ufsm.br:8080/xmlui/bitstream/handle/1/187/Stefanello_Andre_Luis.pdf?sequence=1&isAllowed=y>. Acesso em: 21 mai. 2017.

TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina; ALMEIDA, Vitor (Coords.). **O direito civil entre o sujeito e a pessoa**: estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. 488 p. ISBN 978-85-450-0180-5.

TERRA. **IMPLANTE de chips em funcionários gera polêmica nos EUA**. Publicado em: 20 fev. 2006. Disponível em:< http://tecnologia.terra.com.br/interna/0,,OI886717-EI4799,00-Implante+de+chips+em+funcionarios+gera+polemica+nos+EUA.html >. Acesso em: 12 maio 2017.

VEJA.COM.**Biochip, você ainda vai usar um**. Disponível em: <http://veja.abril.com.br/tecnologia/biochip-voce-ainda-vai-usar-um>. Acessoem: 26 maio 2017.

WARREN, Samuel D.; BRANDEIS, Louis D. **The right to privacy**. Harvard Law Review: Boston, v. 4, n. 5, p. 193-200, dez. 15, 1890, p. 201.

Recebido em: 16-11-2017
Aprovado em: 2-2-2017

Liliane Gonçalves Matos

Mestranda em Direito Constitucional com ênfase nas Relações Privadas, pela Universidade de Fortaleza - UNIFOR. (2012); especialista em Direito e Processo Empresarial pela Universidade de Fortaleza - UNIFOR. (2016); especialista em Direito e Processo Tributário pela Universidade de Fortaleza – UNIFOR (2014); advogada; professora da Faculdade Paraiso do Ceara, da Universidade de Fortaleza e do Centro Universitário Christus. E-mail: liliane.mat@hotmail.com

Universidade de Fortaleza, Conselho de Ensino, Pesquisa e Extensão. Washington Soares, 1321. Edson Queiroz. 60811-905 - Fortaleza, CE.

Joyceane Bezerra de Menezes

Pós-Doutora em Direito Civil pela Universidade do Estado do Rio de Janeiro; doutorado em Direito pela Universidade Federal de Pernambuco; mestrado em Direito Constitucional (Direito e Desenvolvimento) pela Universidade Federal do Ceará; professora titular da Universidade de Fortaleza, integrando o Programa de Pós-Graduação Stricto Sensu em Direito; professora adjunto, nível 4, da Faculdade de Direito da Universidade Federal do Ceará; advogada. E-mail: joyceane@unifor.br

Universidade de Fortaleza, Programa de Pós-Graduação Stricto Senso em Direito. Av. Washington Soares, 1321. Edson Queiroz - 60000000 - Fortaleza, CE - Brasil

Hian Silva Colaço

Mestre em Direito Constitucional nas Relações Privadas pela Universidade de Fortaleza (UNIFOR); especialista em Direito e Processo Constitucionais pela Universidade de Fortaleza; pesquisador na Área de Direito Civil-Constitucional, Direitos de Personalidade, Responsabilidade Civil e Direito Digital; integrante do Grupo de Pesquisa Cnpq - Direito Constitucional nas Relações Privadas. E-mail: hiancolaco@hotmail.com

Tribunal de Justiça do Estado do Ceará - Av. Gal Afonso Albuquerque Lima - Cambeba, CE, 60830-120do Estado do Ceará, TJCE,