13º Concurso de Monografia 'Levy & Salomão Advogados'

INTERNET DAS COISAS: REPERCUSSÕES JURÍDICAS DE UMA REVOLUÇÃO NA DINÂMICA DAS INFORMAÇÕES

André Nunes Conti
Faculdade de Direito da Universidade de São Paulo
Segundo ano

INTERNET DAS COISAS: REPERCUSSÕES JURÍDICAS DE UMA REVOLUÇÃO NA DINÂMICA DAS INFORMAÇÕES

RESUMO

A presente monografia almeja apresentar um panorama dos desafios que o advento da revolução tecnológica conhecida como "Internet das Coisas" traz para o ambiente jurídico. Esses "desafios" são dilemas e questionamentos de duas espécies, com que depara o jurista que procura entender como o ordenamento jurídico se relaciona com as mudanças operadas pela internet das coisas. Por um lado, as questões *de lege lata*: como se aplica o ordenamento vigente à nova realidade? Por outro, as *de lege ferenda*: se a aplicação das normas vigentes levar a soluções insatisfatórias, caberiam mudanças no ordenamento? Essas hão de ser as perguntas formuladas nos campos do Direito mais imediatamente afetados pela internet das coisas: a tutela do direito à privacidade e a responsabilidade civil por danos (ligados à difusão das informações envolvidas com o fenômeno tecnológico em questão); e a anulabilidade de negócios jurídicos por erro (ligada à significação jurídica das informações veiculadas via internet das coisas).

ABSTRACT

This paper aims to present an outlook of the challenges that the coming of the technological revolution known as "Internet of Things" brings to the juridical medium. Those "challenges" are dilemmas and questionings of two species, which are encountered by the jurist that endeavors to understand how the law deals with the changes that result from the internet of things. In the one hand, there are the "de lege lata" questions: how does the actual law apply to the new reality? In the other hand, there is the "de lege ferenda" asking: comes it out that the application of the actual rules redound to unsatisfactory solutions, is it opportune to alter the law? Those are going to be the queries formulated on the Law fields most immediately affected by the internet of things: the ward of the privacy's right and the field of torts (both linked with the diffusion of the information encompassed in the technological phenomenon in analysis); and the invalidity of juridical acts due to error (affined to the juridical significance of the information circulating through the internet of things).

SUMÁRIO.

INTRODUÇÃO

O século XXI trouxe consigo revoluções tecnológicas que mudaram radicalmente o modo das pessoas de interagirem com o mundo e se comunicarem entre si. Uma dessas revoluções vem chamando especialmente a atenção dos pesquisadores: as tecnologias de captação e transmissão de informações têm alcançado níveis assombrosos, alcançando um desempenho excepcional a custos cada vez mais baixos, e repercutindo não só no âmbito da indústria e da ciência, mas também no dia-a-dia dos cidadãos comuns[1].

Nos últimos anos, esse desenvolvimento chegou a um novo patamar, apresentando resultados antes inconcebíveis no que diz respeito à capacidade humana de conhecer seu entorno e de se comunicar com os outros, e gerando expectativas entusiásticas que, a despeito de sua audácia, passam a ser encaradas como realizáveis.

Tornam-se verossímeis ideias como relógios que medem os batimentos cardíacos e informam automaticamente o ar condicionado de que convém diminuir a temperatura ambiente. Aparelhos de ar condicionado, por sua vez, que detectam o desgaste de peças internas e realizam imediatamente pedido de compra para reposição via internet. Carros que, percebendo pelo GPS a proximidade do domicílio, enviam sinais às *smart houses*, que têm suas luzes e um som ambiente instantaneamente acionados. Tênis de corrida contendo sensores que aferem com precisão os dados relativos a uma performance esportiva, lançando-os em uma plataforma *online* que permite a comparação entre corredores de todas as partes do mundo.

Esse fenômeno de crescimento vertiginoso na capacidade de captação, processamento, e troca de informações pelos objetos e utensílios mais banais recebeu o nome de "Internet das Coisas", ou "*Internet of Things*" (*IoT*[2]), em inglês[3]. Kevin Ashton, empreendedor britânico que forjou a expressão em 1999, referia-se com ela à capacidade dos computadores de captar informações por conta própria, sem a ajuda dos humanos[4]. Hoje ela é usada popularmente para descrever o cenário em que a internet se torna acessível via objetos do cotidiano[5] – que se tornam capazes de enviar e receber informações, inserindo-se em uma rede coordenada de funcionamento conjunto. Prevê-se que as aplicações da *IoT* sejam ampliadas nos próximos

---

[1] CULLER, David; ESTRIN, Deborah; TRIVASTAVA, Mani. **Overview of sensors networks**. *IEEE Computer Society*, 2004.
[2] Ao longo desse trabalho, será usada a sigla "*IoT*" toda vez que se fizer referência à internet das coisas.
[3] ROY WANT, Bill N. Schilit; JENSON, Scott. **Enabling the Internet of Things**. *IEEE Computer Society*, 2015.
[4] ASHTON, Kevin. **That 'internet of things' thing**. *RFiD Journal*, jul. 2009, pp. 97-114.
[5] MULANI, Tanjim T.; PINGLE, Subash V.. **Internet of Things**. *International Research Journal of Multidisciplinary Studies*, mar. 2016.

anos, até que cheguem a permear o cotidiano de todos, trazendo melhoras para a qualidade de vida, mas apresentando riscos que não podem ser ignorados[6].

É evidente que essa revolução tecnológica há de causar um impacto considerável de teor econômico, político e – é a perspectiva do presente trabalho – jurídico. Para o Direito, a relevância do fenômeno da *IoT* reside na metamorfose que ele tende a imprimir na dinâmica informacional. Duas são as características das informações que causam extraordinária repercussão no ambiente jurídico: a *possibilidade de serem difundidas* e a de *assumirem significados relevantes para o Direito*. Com a explosão quantitativa (número) e qualitativa (precisão e amplitude) do volume de informações que circula via internet, a *IoT* aprofundou essas características das informações veiculadas *online*, suscitando questões relativas como tratar juridicamente essa hipertrofia informacional.

Quanto à *passividade de difusão*, é sabido que o sistema de *IoT* lida com um volume descomunal de informações qualitativamente muito precisas e quantitativamente muito numerosas, captado autônoma e continuamente. Toda essa massa de informações é processada, tonando-se compreensível e utilizável, e depois veiculada por meio da internet.

Ora, a internet é um espaço virtual comum, a que todos têm acesso para compartilhar informações. É parte essencial da dinâmica da *IoT* o uso comum (ainda que anônimo) das informações captadas – de modo similar a como sistemas de GPS colaborativos, como o conhecido "*Waze*", funcionam com base em dados coletados de todos os usuários[7]. Assim, as inúmeras informações pessoais dos usuários são mantidas em um ambiente público – e, portanto, acessível. Mesmo que se mantenham ocultas ou criptografadas, sob um regime de uso privado, o fato de estarem na internet faz impossível tirá-las do alcance de ao menos três sujeitos: o próprio *software* que as administra, o Estado e os *Hackers*. As implicações jurídicas da possibilidade de acesso a essas informações por esses três sujeitos, no âmbito da proteção à privacidade e da responsabilidade civil, serão estudadas na primeira parte do presente trabalho.

Quanto à outra característica das informações envolvidas no sistema de *IoT* que as torna relevantes para o Direito – a sua eventual *significação jurídica* –, cabe pensar nos impactos que a torrente de informações que circula via *IoT* representará para a atividade de interpretação dos negócios jurídicos, cujos vícios e motivação passam a ser muito mais facilmente conhecidos pelo destinatário das declarações de vontade. Nesse sentido, o fenômeno da *IoT* faz com que emerjam questionamentos a respeito da disciplina jurídica do erro como causa de anulabilidade dos negócios jurídicos. Essa análise será o objeto da segunda parte.

---

[6] *Vide* a respeito dos riscos: XIA, Feng, et al., **Internet of things**. *International Journal of Communication Systems*, set. 2012, p. 1101.

[7] ROY WANT, Bill N. Schilit; JENSON, Scott. **Enabling the Internet of Things**. Op. cit. nt. 3 *supra*.

Vale frisar: o que se pretende com este estudo é apresentar um panorama de alguns dos impactos que o advento da *IoT* há de causar no ambiente jurídico. É certo que as múltiplas novidades trazidas por esse novo estágio das tecnologias digitais hão de significar verdadeiros desafios para os juristas, que se enfrentarão com questões de duas espécies[8]: *i)* como o ordenamento jurídico vigente se aplica às situações inusitadas que a *IoT* produz (questões *de lege lata*); e *ii)* em que medida são oportunas transformações no ordenamento jurídico, para adaptá-lo à nova realidade, permitindo aproveitar todas as potenciais vantagens do fenômeno da *IoT* (questões *de lege ferenda*). Uma e outra espécie de questionamento serão realizadas ao fim de cada tópico desenvolvido no decorrer do trabalho.

Naturalmente, as proporções do presente estudo obstam a pretensão de solucionar todas essas questões. Os desafios da *IoT* para o meio jurídico serão aqui *apresentados*; suas soluções hão de exigir o esforço conjunto de muitos pesquisadores, e serão desenvolvidas paulatinamente, à medida que se forem aprofundando as transformações operadas pela *IoT*.

[8] Comentando os desafios a serem enfrentados pelo Direito com o advento da internet (não da *IoT*), Marcel LEONARDI (**Tutela e privacidade na internet**. São Paulo: Saraiva, 2012, p. 39) menciona essas duas espécies de questões, chamando atenção para a necessidade de identificar os pontos de estrangulamento do ordenamento vigente, de modo a saber o que reclama mudanças.

PRIMEIRA PARTE: sobre o acesso às informações coletadas via *IoT*.

1. *Softwares* administradores e direito à privacidade.

As informações envolvidas no complexo de componentes da *IoT* são processadas e administradas por meio de *softwares*, que, por sua vez, são produzidos e controlados por grandes empresas, como a *Google*[9]. Essas empresas têm acesso ao conteúdo das informações pessoais que, a todo momento e em todos os lugares, são auferidas dos usuários da *IoT*. O valor econômico desses dados estimula sua exploração comercial: assim como o *facebook* vende a empresas de publicidade informações usadas para determinar os anúncios que serão exibidos nas páginas de seus usuários[10], os *softwares* que operam os dados do sistema de *IoT* podem almejar vantagens econômicas com a sua venda.

Note-se que esse intercâmbio de informações pode até ser benéfico ao usuário da *IoT*. Com efeito, análise precisa e sistemática de todas as informações colhidas permite aos *softwares* descobrir necessidades reais de que nem mesmo o interessado tinha conhecimento: refis para a máquina de café, um par de tênis ortopédicos que evitem lesões, um computador novo dotado de potência compatível com a habitualmente exigida, etc.

Entretanto, é patente o risco que esse monitoramento representa para a privacidade das pessoas[11]. Já em 2001, quando ainda incipiente a prática de manipulação dos dados acumulados com o uso normal de um *software*, J. S. STHELL alertava: "As novas tecnologias transformam numa coisa banal a espionagem dos indivíduos em todos os campos da vida cotidiana"[12]. Dado o particular caráter intrusivo da captação de informações no âmbito da *IoT* – que alcança as pessoas mesmo em suas casas, acompanhando-as no seu dia-a-dia – essa afronta à privacidade sofre evidente agravo.

---

[9] Como exemplo, vejam-se os esperados *Google Cars* – carros que operam sem motorista, via internet. BBC. **Legal breakthrough for Google's self-driving car**, 17/08/2016, disponível em http://www.bbc.co.uk/news/technology-35539028 (acesso em 16/10/2016, às 19:12), ou o *Google Glass*.

[10] *Vide* a respeito: RIEDERER, Christopher et al. **For sale: your data: by: you in: Proceedings of the 10th ACM WORKSHOP on Hot Topics in Networks**. ACM, 2011, p. 13.

[11] SANTOS, Carlos Cesar; ARAÚJO SALES, Jefferson David de. **O Desafio da Privacidade na Internet das Coisas**. *Revista Eletrônica de Gestão Organizacional n. 13*, 2016. Os autores destacam quatro formas de violação da privacidade no âmbito da *IoT*: coleta, disseminação, divulgação e invasão de informações.

[12] STHELL, Jean-Sebastian. **Ameaça a nossa vida privada**, trad. José dos Santos. *O Estado de São Paulo*, Caderno 2, 18/03/2001, p, D10. A respeito das ameaças que o advento da internet oferece ao direito à privacidade, *vide* BITTAR, Carlos Alberto. **Os direitos da personalidade**, 8ª ed., rev., ampl. e mod. São Paulo: Saraiva, 2015, p. 178 – 180.

E maior ameaça ainda é representada pela cessão desses dados a terceiros, que os utilizem para fins comerciais, como publicidade seletiva. Há quem a considere ilícita sempre que não autorizada pelo interessado – por força do chamado "princípio da finalidade", que restringe a utilização dos dados pessoais aos fins previamente convencionados[13]. Mesmo consentida, porém, essa devassa do foro privado pode ser questionada: sendo a privacidade, enquanto direito fundamental (art. 5º, X, CF) e direito da personalidade (art. 21, CC), indisponível[14] (por mais que possa sofrer restrições, queridas por seu titular e expressas em documento hábil[15]), é duvidosa a licitude de sua renúncia geral e absoluta por quem se introduz em um contexto de exposição da própria intimidade que foge ao seu controle. Ainda mais: a dinâmica de funcionamento da *IoT* pode ser até mesmo incompatível com a celebração de um acordo prévio a cada cessão: se fosse exigido o consentimento expresso a todo momento, a *IoT* seria destituída da instantaneidade e da automaticidade que fazem parte de sua essência.

Atualmente, o direito à privacidade[16] é protegido clara e taxativamente pela norma do art. 5º, X, da Constituição Federal, que estabelece o dever de indenizar para quem viola a "vida privada" ou a "intimidade"[17] de outrem.

Apresentam-se, assim, questões jurídicas importantes.

De lege lata, cabe perguntar: a cessão de informações captadas via *IoT* a terceiros, que pode chegar a ser realmente benéfica ao interessado, é compatível com a proteção constitucional à privacidade[18]? Mesmo sendo benéfica, exige sempre o expresso consentimento do interessado? Não é parte essencial da dinâmica da *IoT* essa cessão de informações? Não há um consentimento tácito, com essa cessão, de quem passa a utilizar essa tecnologia?

---

[13] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 216.

[14] Como deixa expresso o art. 11 do Código Civil, que estabelece a irrenunciabilidade dos direitos da personalidade, "não podendo seu exercício sofrer limitação voluntária", exceto nos casos previstos em lei. Como na lei não está prevista essa hipótese, o direito à privacidade é irrenunciável. Note-se a diferença: exercer o direito à privacidade como faculdade, optando pela divulgação de determinadas informações, é prática absolutamente legítima. Dispor desse direito, contudo, limitando voluntariamente seu exercício (por entrar em um contexto em que os dados relativos à intimidade saem do próprio controle) é contrário ao art. 11, CC.

[15] BITTAR, Carlos Alberto. **Os direitos.** Op. cit. nt. 12 *supra*, p. 174.

[16] O conteúdo desse direito é definido com precisão em SILVA, José Afonso da. **Curso de direito constitucional positivo**. 20ª ed., São Paulo: Malheiros, 2002, pp. 204 – 209, e em MORAES, Alexandre de. **Direitos humanos fundamentais: teoria geral, comentários aos arts. 1o a 5o da Constituição da República Federativa do Brasil, doutrina e jurisprudência.** 3ª ed. São Paulo: Atlas, 2000, pp. 135 e 136.

[17] Para uma reflexão interessante a respeito da distinção entre "privacidade" e "intimidade", *vide* ALONSO, Félix Ruiz. **Pessoa, Intimidade e o Direito à Privacidade.** In: MARTINS, Ives Gandra da Silva; PEREIRA JR., Antônio Jorge (Org.), **Direito à Privacidade**. São Paulo: Centro de Extensão Universitária, 2005, pp. 11-35.

[18] A questão envolve a cessão de informações no âmbito da *IoT*, ou seja, em um âmbito em que essa prática, pelo volume e pela qualidade das informações cedidas, é mais grave que no contexto anterior à *IoT* – em que já é amplamente praticada. *Vide* SANTOS, Carlos Cesar; ARAÚJO SALES, Jefferson David de. **O Desafio**. Op. cit. nt. 12 *supra*.

E, em não sendo compatíveis essa prática e a legislação atual, seria possível, *de lege ferenda*, atenuar a literalidade do inciso X do art. 5º da Carta Magna, a bem dos benefícios decorrentes dessa nova dinâmica informacional, sem desrespeitar seu *status* de cláusula pétrea[19]? Quais seriam as especificações legislativas cabíveis, direcionadas a estabelecer os limites dessa prática, evitando que se tornasse prejudicial?

As respostas não são triviais, e exigem estudos aprofundados a respeito.

2. A *IoT* e as provas ilícitas.

É conhecida a tensão permanente entre a eficácia da atividade probatória e o respeito aos direitos e garantias fundamentais. O ordenamento jurídico brasileiro, privilegiando os direitos fundamentais, determina serem ilícitas – e, portanto, inadmissíveis no processo[20] – as provas colhidas com sua violação (art. 5º, LVI, CF) [21]. Assim, são ilícitas as provas obtidas com a violação do direito à privacidade (art. 5º, X, CF) ou às inviolabilidades de domicílio (art. 5º, XI, CF), de correspondência e de comunicações telegráficas ou telefônicas (art. 5º, XII, CF)[22]. Por analogia, aplica-se essa proteção às comunicações telemáticas e aos dados pessoais[23].

Existe, contudo, uma exceção às inviolabilidades do art. 5º, XII da Constituição – estabelecida por esse mesmo dispositivo: por ordem judicial, podem ser violadas as comunicações telefônicas para fins de investigação penal ou instrução processual penal.

Com o advento da *IoT*, surgem problemas complexos relacionados ao tema. O volume e a qualidade das informações que circulam via internet entre os componentes do sistema da *IoT* podem conferir uma eficiência sem precedentes à investigação probatória. Prevendo num futuro próximo a generalização e a consolidação do uso de objetos conectados à internet e capazes de colher informações, o Estado terá à sua disposição um banco de dados impressionante contendo informações minuciosas relativas a todos os cidadãos – inclusive a

---

[19] Atentando para o fato de que o art. 60, § 4º, IV da Constituição Federal impede a deliberação de emenda "tendente a abolir" direitos e garantias fundamentais, e não de emenda voltada à adaptação dos direitos e garantias fundamentais à realidade social (sempre mutável).

[20] Exceto no processo penal, quando levem à absolvição do réu (MORAES, Alexandre. **Constituição do Brasil Interpretada e Legislação Constitucional**. 5ª ed. São Paulo: Atlas, 2005, p. 386).

[21] MORAES, Alexandre. **Constituição**. Op. cit. nt. 20 *supra*, p. 386. No mesmo sentido, BALTAZAR JR., José Paulo. **Limites constitucionais à investigação. O conflito entre o direito fundamental à segurança e o direito de liberdade no âmbito da investigação criminal**. In: CUNHA, Rogério Sanches; TAQUES, Pedro; GOMES, Luiz Flávio. **Limites constitucionais da investigação**, São Paulo, Ed. RT, 2009, pp. 184 – 221.

[22] MORAES, Alexandre. **Constituição**. Op. cit. nt. 20 *supra*, pp. 386 – 389.

[23] MORAES, Alexandre. **Constituição**. Op. cit. nt. 20 *supra*, pp. 240 – 251.

suspeitos criminosos. Será grande a tentação de utilizar irrestritamente essa ferramenta como catalisadora da atividade probatória – mesmo com a decorrente afronta a direitos fundamentais.

Como se disse, os dados pessoais, assim como as comunicações telemáticas, entram, por analogia, na proteção do art. 5º, XII, da Constituição. A princípio, portanto, não seriam admissíveis no processo as provas colhidas com o acesso ao banco de dados que a *IoT* proporciona. Entretanto, cabe perguntar se a exceção do art. 5º, XII, também se aplica a esses dados: poderia o Estado, por ordem judicial, autorizar a invasão dessas informações para fins de investigação ou instrução processual penal? Note-se que a questão não é simples. P. B. MARCHETTO defende que a exceção do art. 5º, XII, deva-se aplicar restritamente às comunicações telefônicas, não abrangendo a violação de dados[24]. Mas essa interpretação não é a única possível, e o dilema persiste. Se, por um lado, já vêm sendo dadas ordens judiciais para a violação de comunicações telemáticas[25] e é sabido o extraordinário potencial de eficácia probatória dos dados veiculados no âmbito da *IoT*, por outro, o caráter excessivamente intrusivo das dessa informações pode reclamar para esses dados uma proteção especial.

Mais uma vez, caberá ao Direito buscar o equilíbrio entre dois valores importantíssimos: a privacidade e a eficiência probatória.

Em primeiro lugar, cabe perguntar: *de lege lata*, a exceção do inciso XII do art. 5º da Carta Magna será aplicável às informações que circulam nos ambientes virtuais da *IoT*, a bem da extraordinária eficácia probatória que esses dados oferecem? Isso mesmo em face da particular extensão (quantitativa e qualitativa) dessas informações, que agrava consideravelmente a violência sofrida pela privacidade do interessado?

E, em não sendo aplicável a exceção do inciso XII, seria porventura possível (*de lege ferenda*) alterar a legislação constitucional, especificando a disciplina a ser aplicável na hipótese de violação dos dados envolvidos no sistema de *IoT*?

3. Os *hackers* e a responsabilidade civil na internet.

[24] MARCHETTO, Patricia Borba. **El derecho a la intimidad y las pruebas ilicitamente obtenidas**. Bauru: Canal 6, 2007, p. 164 e 165. Apesar do título espanhol, parte do estudo toma por objeto a Constituição Federal do Brasil.
[25] Como nos recentes casos de ordens dirigidas ao WhatsApp para a divulgação de informações concernentes ao processo. *Vide*, por exemplo, FOLHA DE SÃO PAULO. **WhatsApp é bloqueado no Brasil após decisão judicial**, 19/07/2016, disponível em http://www1.folha.uol.com.br/mercado/2016/07/1793221-whatsapp-comeca-a-ser-bloqueado-no-brasil-apos-decisao-judicial.shtml (acesso em 19/10/2016, às 9:25).

A despeito dos mecanismos de segurança constantemente desenvolvidos com o objetivo de proteger os usuários da internet da invasão de seus dados por *experts* em informática, casos recentes como os do *site Wikileaks*[26] demonstram sempre haver riscos de acesso por terceiros a quaisquer dados veiculados na internet. Agravados pela própria natureza da *IoT*, que lida com um volume colossal de informações mantidas na internet, esses riscos devem ser suportados por alguém – na hipótese de os causadores do dano não serem identificados. Os danos podem ser graves: uma invasão no sistema de *IoT* que dê acesso a informações como "sistema elétrico da casa no modo economia de energia" podem sinalizar a ausência dos moradores, facilitando a prática de crimes como o assalto[27]. Daí decorre a questão da responsabilidade por danos[28] no contexto da *IoT*.

I. G. da S. MARTINS defende que as violações de dados por quebra de sistemas de segurança não devem ensejar ações reparatórias, por faltar a intenção de torná-los públicos[29]. Não haveria sequer negligência (e, portanto, culpa) das empresas que produzem e administram os *softwares* componentes da *IoT*. Excluir-se-ia, assim, a possibilidade de exigir reparação com base no art. 186 do Código Civil, combinado com o *caput* do art. 927 do mesmo Código (responsabilidade subjetiva[30]).

Entretanto, cabe levantar a possibilidade de subsumir a atividade das empresas de *softwares*, no âmbito da *IoT*, ao Parágrafo Único do mesmo art. 927, que estabelece o dever de indenizar o dano independentemente de culpa (responsabilidade objetiva[31]) quando a atividade desenvolvida pelo agente implicar, por sua natureza, risco para os direitos de outrem. Conforme visto, a natureza da *IoT* implica riscos mais elevados que o ordinário: há mais informações potencialmente violadas, cuja violação apresenta caráter especialmente intrusivo na vida

---

[26] BBC. **What is Wikileaks?**, 07/12/2010, disponível em http://www.bbc.com/news/technology-10757263 (acesso 14/10/2016, às 16:49).

[27] ROY WANT, Bill N. Schilit; JENSON, Scott. **Enabling the Internet of Things**. Op. cit. nt. 3 *supra*. Isso sem falar na possibilidade de controle remoto dos objetos integrados no sistema de *IoT* via internet. Um *hacker* que assuma o controle de um carro sem motorista conectado à internet pode causar danos gravíssimos.

[28] Para um panorama a respeito da responsabilidade por danos causados por *hackers* no contexto da internet, *vide* VANCIM, Adriano Roberto; MATIOLI, Jefferson Luiz. **Direito e Internet – Contrato Eletrônico e Responsabilidade Civil na Web**. Leme: Lemos e Cruz, 2011, pp. 99 – 102.

[29] MARTINS, Ives Gandra da Silva; MARTINS, Rogério Vidal Gandra da Silva, **Privacidade na Comunicação Eletrônica** in GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Org.). **Direito e Internet - Relações Jurídicas na sociedade informatizada**. São Paulo: Ed. RT, 2001, p. 52.

[30] RODRIGUES, Silvio. **Direito civil – Vol. 4 – Responsabilidade civil.** 18ª ed. rev. São Paulo: Saraiva, 2000, p. 11, e COSTA, Fernanda Serra de Souza. **Responsabilidade Civil: um breve sumário de suas principais classificações doutrinárias** In: ALMEIDA GUILHERME, Luiz Fernando do Vale de. **Responsabilidade Civil II**. São Paulo: Fiuza, 2013, p. 141.

[31] RODRIGUES, Silvio. **Direito**. Op. cit. nt. 30 *supra*; MOURA, Cristina A. O. R. **Responsabilidade civil nas atividades perigosas: o paradigma do Código Civil italiano e o novo Código Civil brasileiro** In: HIRONAKA, Giselda Maria Fernandes Novaes, FALAVIGNA, Maria Clara Osuna Diaz. **Ensaios sobre a responsabilidade civil na pós-modernidade**. Porto Alegre: Magister, 2007, pp. 64 – 68.

privada do atingido. Será possível, então, eximindo os usuários de suportar riscos demasiado onerosos, imputar objetivamente eventuais danos às empresas que tiverem seus *softwares* invadidos por *hackers* que quebrem seus sistemas de segurança[32]?

É preciso, também, enfrentar a questão relativa às cláusulas de extinção ou diminuição da responsabilidade[33]. Não parece possível admitir cláusulas que visem a eximir completamente de responsabilidade os causadores do dano: as regras dos art. 186 e 927 são cogentes[34]. A diminuição da responsabilidade, contudo, não é vedada *a priori*[35]. Cabe discutir se o pacto segundo o qual a empresa do *software* invadido será responsável apenas até os limites do estado da técnica configura cláusula abusiva. Tendo em vista a excessiva onerosidade de uma responsabilidade objetiva sem limitações, bem como a necessidade de estimular as empresas que decidem investir em tecnologias de *IoT*, pode ser oportuno admitir cláusulas que reduzam aos limites do razoável a responsabilidade por danos. São questionamentos à espera de respostas.

SEGUNDA PARTE: sobre a significação jurídica das informações coletadas via *IoT*.

4. A relevância da vontade real do declarante.

A repercussão da *IoT* no ambiente jurídico decorrente da possível significação jurídica de suas informações é menos evidente que a já analisada repercussão ligada à ao risco de difusão indesejada dos dados pessoais. Assim mesmo, afigura-se conveniente tratar dela com minúcia, buscando pôr em relevo um aspecto importante do fenômeno tecnológico em questão: a possibilidade de lançar mão dos dados veiculados via *IoT* para interpretar as *declarações* jurídico-negociais em busca da real *vontade* do declarante.

---

[32] *Vide* a respeito: LOTUFO, Renan. **Responsabilidade Civil na Internet.** In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva. **Direito e Internet - Relações Jurídicas na sociedade informatizada**. São Paulo: Ed. RT, 2001, pp. 235. Sem tratar da Internet das Coisas, o autor discorre sobre a conveniência da responsabilidade objetiva como técnica para a distribuição dos riscos no contexto da internet em geral.
[33] *Id., ibid.*
[34] *Id., ibid.*
[35] *Id., ibid.*

Evidentemente, não se trata de procurar conhecer uma vontade absolutamente interna, puramente subjetiva: o que não é objetivado e não se torna parte da relação intersubjetiva é irrelevante para o Direito – fenômeno eminentemente social[36].

O Direito, contudo, não ignora a vontade interna (conteúdo da declaração) quando objetivada, cognoscível. Embora não afete o plano da *existência* dos negócios jurídicos, para cuja configuração basta a declaração jurídico-negocial[37], a real vontade de quem declara repercute nos planos da *validade* e *eficácia*[38], sendo relevante no que concerne à anulabilidade por vícios[39] e à interpretação[40] dirigida a determinar o conteúdo do negócio.

5. As informações no âmbito da *IoT* e a anulabilidade dos negócios por erro.

Dentre os possíveis defeitos do negócio jurídico, destaca-se o erro, que consiste em uma falsa representação psicológica da realidade[41]. Disciplinado pelos art. 138 a 144 do Código Civil, o erro é causa de anulabilidade do negócio jurídico quando apresentar dois requisitos: substancialidade e cognoscibilidade[42]. Esse segundo requisito é previsto no art. 138, CC, cuja redação faz referência ao erro que "poderia ser percebido por pessoa de diligência normal, em face das circunstâncias do negócio" (o destinatário da declaração que funda negócio viciado por erro tem o dever de informar o juízo errôneo que percebe).

Com o advento da *IoT*, a dinâmica da troca de informações entre as partes de um contrato (negócio jurídico bilateral[43]) sofre profundas alterações. No âmbito dos contratos celebrados pela internet, cada um dos contratantes tem acesso a um volume de dados sem

---

[36] PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de Direito Privado – Vol. I – Introdução. Pessoas físicas e jurídicas.**, at. MARTINS-COSTA, Judith; HAICAL, Gustavo; FERREIRA DA SILVA, Jorge Cesa, São Paulo: Ed. RT, 2013, (§ 25) p. 152. MELLO, Marcos Bernardes de. **Teoria do fato jurídico – plano da validade**. 4ª ed. rev. São Paulo: Saraiva, 2000, p. 115.

[37] As declarações jurídico-negociais, ou declarações de vontade, são definidas por PONTES DE MIRANDA (**Direito**. Op. cit. nt. 36 *supra*) como "as exteriorizações da vontade, aptas de serem elemento de suporte fático de fato jurídico, com ou sem o intuito de se ter eficácia jurídica de tal fato". A expressão "com ou sem o intuito de se ter eficácia jurídica de tal fato" faz referência ao "intuito" do declarante, sua vontade interna: essa, de fato, não impede – mesmo que vindo a faltar – a existência do negócio. Basta a declaração, a exteriorização material.

[38] AZEVEDO, Antônio Junqueira de. **Negócio jurídico: existência, validade e eficácia**. 4ª ed. São Paulo: Saraiva, 2002. (7a tiragem, 2010), pp. 74 – 87; MELLO, Marcos Bernardes de. **Teoria do fato jurídico – plano da existência**. 16ª ed. São Paulo: Saraiva, 2010, p. 173; MELLO, Marcos Bernardes de. **Teoria**. Op. cit. nt. 36 *supra*, p. 116.

[39] Art. 171, II, CC.

[40] Art. 110 – 114, CC.

[41] MELLO, Marcos Bernardes de. **Teoria**. Op. cit. nt. 36 *supra*, p. 117.

[42] Existem discussões a respeito de um terceiro requisito: que o erro seja escusável, compreensível. MELLO (**Teoria**. Op. cit. nt. 36 *supra*, p. 117), por exemplo, sustenta não ser esse um verdadeiro requisito. Para fins do que aqui se busca demonstrar, essa discussão não é relevante.

[43] PEREIRA, Caio Mário da Silva. **Instituições de direito civil**. 4ª ed. Rio de Janeiro: Forense, 1978, p. 10.

precedentes relativos à outra parte. Como consequência, passam a ser "cognoscíveis" (para a pessoa de diligência "normal") eventuais erros que, antes da *IoT*, jamais teriam podido ser conhecidos. Com efeito, o "normal" é aferido em conformidade com as possibilidades técnicas generalizadas nas circunstâncias sociais em que o negócio é realizado; com a facilidade de acesso às informações captadas, processadas e veiculadas via *IoT*, passa a ser "normal" – embora nem sempre trivial – a percepção de erros antes fora do alcance de pessoa diligente.

Assim, passa a ser cognoscível o erro de quem compra, via internet, peça de reposição incompatível com a sua geladeira – que, conectada à internet, deixa à disposição do vendedor as informações relativas a seu modelo. Do mesmo modo, torna-se cognoscível o erro de quem solicita o serviço de *Uber* na modalidade "carro padrão", quando seria necessário um carro com espaço extra para bagagem, se as malas de quem comete o erro – por estarem conectadas à internet – deixarem à disposição do sistema *Uber* a real necessidade do declarante.

Essa facilidade de atendimento ao requisito da cognoscibilidade do erro suscita questões jurídicas importantes.

De lege lata, cabe perguntar: é razoável permitir a anulabilidade por erro sempre que, via *IoT*, as informações relativas a esse vício estiverem ao acesso do destinatário da declaração? Quais seriam as consequências dessa permissão? Ela conferirá maior proteção a quem celebra contratos via internet, ou aumentará vertiginosamente a possibilidade de anulação de contratos celebrados nesse âmbito – incrementando consideravelmente a insegurança jurídica? Se o até menor e mais sutil erro for amparado pela norma do art. 138, ninguém – nem mesmo quem empregue "diligência normal" – poderá celebrar contratos via internet sem assumir o risco de sua posterior anulação por erro. Nesse sentido, o advento da *IoT* exige uma interpretação cuidadosa da expressão "diligência normal" usada pelo Código Civil. O normal pode se tornar pouco razoável, e normalizar a insegurança jurídica.

De lege ferenda, a *IoT* pode dar ensejo à reformulação do art. 138, CC, que determine com maior clareza ser anulável o erro cognoscível para pessoa com diligência "razoável" – limitando a incidência da norma aos casos em que a anulabilidade não resultar em excessivo risco para o outro contratante.

CONCLUSÃO.

Feitas todas essas análises, fica evidente que a "internet das coisas", alterando radicalmente a dinâmica da circulação das informações, apresenta uma série de desafios para os juristas. Esses desafios consistem em dilemas com que depara quem procura responder a perguntas de duas espécies: *i)* (*de lege lata*) o ordenamento jurídico vigente se aplica de modo adequado às novas situações que a *IoT* proporciona?; *ii)* (*de lege ferenda*) se não forem adequadas as soluções já existentes, convém criar novas, operando as necessárias mudanças na lei?

Dividindo em dois âmbitos o impacto que a *IoT* causa na dinâmica informacional, é possível falar de dois gêneros de desafios que essa revolução tecnológica apresenta ao Direito.

Por um lado, surgem as questões ligadas à possibilidade de difusão da torrente de informações colhidas, processadas e veiculadas via *IoT*. Nesse sentido, cabe perguntar: em que medida o direito à privacidade, tal como é hoje protegido, seria violado pela venda de dados pessoais dos usuários da *IoT* pelos controladores dos *softwares* que operam o sistema, ou pela admissão, no processo penal, de provas extraídas do banco de dados da *IoT*, que permitiria conhecer tudo sobre determinados suspeitos? E como se aplicam as normas ligadas à responsabilidade civil (subjetiva ou objetiva, com ou sem cláusula de redução de responsabilidade) aos danos causados por *hackers* no contexto da *IoT*? E, ainda, se as respostas fossem negativas, seriam desejáveis mudanças legais?

Por outro lado, emergem os questionamentos concernentes à possível significação jurídica dos comportamentos humanos captados e veiculados via *IoT*: é exigível das partes que tomem conhecimento da massa de informações que a *IoT* lhes disponibiliza? Sendo exigível esse conhecimento, o erro que dá ensejo à anulação do negócio passa a atender muito mais facilmente ao requisito da "cognoscibilidade", donde emerge a questão: isso não pode acarretar um excesso de insegurança jurídica? Conviria alterar a redação dos dispositivos legais concernentes ao erro, de modo a deixar clara uma interpretação que favoreça a segurança jurídica?

Todas essas dúvidas configuram alguns dos grandes desafios que, na era da internet das coisas, o Direito terá de enfrentar.

REFERÊNCIAS BIBLIOGRÁFICAS.

ALMEIDA GUILHERME, Luiz Fernando do Vale de (Org.). **Responsabilidade Civil II**. São Paulo: Fiuza, 2013.

ASHTON, Kevin. **That 'internet of things' thing.** *RFiD Journal*, jul. 2009, pp. 97-114.

AZEVEDO, Antônio Junqueira de. **Negócio jurídico: existência, validade e eficácia**. 4ª ed. São Paulo: Saraiva, 2002. (7a tiragem, 2010).

BBC. **Legal breakthrough for Google's self-driving car**, 17/08/2016, disponível em http://www.bbc.co.uk/news/technology-35539028 (acesso em 16/10/2016, às 19:12).

BBC. **What is Wikileaks?**, 07/12/2010, disponível em http://www.bbc.com/news/technology-10757263 (Acesso 14/10/2016, às 16:49).

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8ª ed., rev. ampl. e mod. São Paulo: Saraiva, 2015.

CULLER, David; ESTRIN, Deborah; TRIVASTAVA, Mani. **Overview of sensors networks**. *IEEE Computer Society*, 2004.

CUNHA, Rogério Sanches; TAQUES, Pedro; GOMES, Luiz Flávio (Org.). **Limites constitucionais da investigação**. São Paulo: Ed. RT, 2009.

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

HIRONAKA, Giselda Maria Fernandes Novaes; FALAVIGNA, Maria Clara Osuna Diaz (Org.). **Ensaios sobre a responsabilidade civil na pós-modernidade**. Porto Alegre: Magister, 2007.

FOLHA DE SÃO PAULO. **WhatsApp é bloqueado no Brasil após decisão judicial**, 19/07/2016, disponível em http://www1.folha.uol.com.br/mercado/2016/07/1793221-

whatsapp-comeca-a-ser-bloqueado-no-brasil-apos-decisao-judicial.shtml (acesso em 19/10/2016, às 9:25).

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

LOTUFO, Renan. **Responsabilidade Civil na Internet** In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Org.), **Direito e Internet - Relações Jurídicas na sociedade informatizada**. São Paulo: Ed. RT, 2001.

MARCHETTO, Patricia Borba. **El derecho a la intimidad y las pruebas ilicitamente obtenidas**. Bauru: Canal 6, 2007.

MARTINS, Ives Gandra da Silva; MARTINS, Rogério Vidal Gandra da Silva, **Privacidade na Comunicação Eletrônica**. In: GRECO, Marco Aurélio; MARTINS, Ives Gandra da Silva (Org.), ***Direito e Internet - Relações Jurídicas na sociedade informatizada***. São Paulo: Ed. RT, 2001.

MELLO, Marcos Bernardes de. **Teoria do fato jurídico – plano da existência**. 16ª ed. São Paulo: Saraiva, 2010.

MELLO, Marcos Bernardes de. **Teoria do fato jurídico – plano da validade**. 4ª ed. rev. São Paulo: Saraiva, 2000.

MORAES, Alexandre. **Constituição do Brasil Interpretada e Legislação Constitucional**. 5ª ed. São Paulo: Atlas, 2005.

MORAES, Alexandre de. **Direitos humanos fundamentais: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência**. 3ª ed. São Paulo: Atlas, 2000.

MULANI, Tanjim T.; PINGLE, Subash V. **Internet of Things**. *International Research Journal of Multidisciplinary Studies*, mar. 2016.

PEREIRA, Caio Mário da Silva. **Instituições de direito civil**. 4ª ed. Rio de Janeiro: Forense, 1978.

PONTES DE MIRANDA, *Francisco Cavalcanti*. **Tratado de Direito Privado – Vol. I – Introdução. Pessoas físicas e jurídicas**. at. MARTINS-COSTA, Judith; HAICAL, Gustavo; FERREIRA DA SILVA, Jorge Cesa. São Paulo: Ed. RT, 2013.

RODRIGUES, Silvio. **Direito civil – Vol. 4 – Responsabilidade civil**. 18ª ed. rev. São Paulo: Saraiva, 2000.

ROY WANT, Bill N. Schilit; JENSON, Scott. **Enabling the Internet of Things**, *IEEE Computer Society*, 2015.

SANTOS, Carlos Cesar; ARAÚJO SALES, Jefferson David de. **O Desafio da Privacidade na Internet das Coisas**, *Revista Eletrônica de Gestão Organizacional*, *n. 13*, 2016.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 20ª ed. São Paulo: Malheiros, 2002.

STHELL, Jean-Sebastian. **Ameaça a nossa vida privada**. trad. SANTOS, José. In: O Estado de São Paulo, Caderno 2, 18/03/2001, p, D10.

VANCIM, Adriano Roberto; MATIOLI, Jefferson Luiz. **Direito e Internet – Contrato Eletrônico e Responsabilidade Civil na Web**. Leme: Lemos e Cruz, 2011.

XIA, Feng et al. **Internet of things**, *International Journal of Communication Systems*, set. 2012, p. 1101.