Revista de Direito, Governança e Novas Tecnologias

DOI: 10.21902/
Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 16.07.2016
Aprovado em: 19.12.2016

OS PROVEDORES DE APLICAÇÃO DE INTERNET E A MITIGAÇÃO DO PRINCÍPIO DA FINALIDADE EM VISTA DA COOPERAÇÃO COM AGÊNCIAS DE INTELIGÊNCIA

INTERNET APPLICATION PROVIDERS AND THE MITIGATION OF THE FINALITY PRINCIPLE IN ORDER OF THE COOPERATION WITH INTELLIGENCE AGENCIES

[1] Juliana Evangelista de Almeida
[2] Daniel Evangelista Vasconcelos Almeida

RESUMO

Muitas das informações que os provedores de aplicação de internet possuem sobre usuários podem ser úteis para a investigação de condutas delituosas. Assim, o artigo se propõe a analisar a conformação do princípio da finalidade e a necessidade dos provedores de aplicação de internet em cooperarem com agências de inteligência. Far-se-á uma análise sobre a égide do ordenamento jurídico brasileiro e comparando os termos de uso e as políticas de privacidade de alguns provedores com esse sistema jurídico.

Palavras-Chave: Princípio da Finalidade; Cooperação; Agências de Inteligência; Termos de Uso; Política de Privacidade.

ABSTRACT

Much of the information that the internet application providers have about users may be useful for the investigation of criminal conduct. Thus, this article aims to analyze the conformation of the finality principle and the requirement for Internet application providers to cooperate with intelligence agencies. It will be made an analysis due the Brazilian legal system and it will be compare the terms of use and privacy policies of some providers with this legal system.

Keywords: Finality Principle; Cooperation; Intelligence Agencies; Terms of Use; Privacy Policy.

[1]Doutoranda em Direito Privado pela Pontifícia Universidade Católica – PUC, Belo Horizonte, Minas Gerais, Bolsa da FAPEMIG, (Brasil). Professora de Direito Civil na FACHI/FUNCESI e na Nova Faculdade; Advogada. E-mail: jualmeidaonline@gmail.com

[2] Mestrando em Direito Privado pela Pontifícia Universidade Católica – PUC, Belo Horizonte, Minas Gerais, (Brasil). Advogado; E-mail: danielevangelista@gmail.com

1 INTRODUÇÃO

Os provedores de serviço na internet possuem uma vasta quantidade de dados pessoais e informações dos usuários. Ante ao avanço da tecnologia, os computadores possuem uma capacidade de processar informação cada vez maior. Assim, é preciso que se discuta o uso de tais informações.

Tratando-se de um provedor de serviço, a relação entre este e o usuário será regulada através de um termo de uso, que nada mais que um contrato de adesão virtual. Assim sendo, o usuário não tem o poder de modificar as cláusulas contratuais, optando por aderir ao serviço ou não, aceitando integralmente as regras. Neste sentido, é preciso que se relativize os efeitos dos contratos, com a invalidade de determinadas cláusulas caso se faça necessário.

Assim sendo, no capítulo 2 será feita a análise do termo de uso em uma abordagem geral. Será trabalhada com a ruptura da preponderância do elemento vontade na relação contratual, o que relativiza os efeitos do contrato. Assim se diz que se contrata em virtude da confiança que o usuário tem no prestador de serviço.

Como há uma vasta gama de informações coletadas pelos provedores de serviço, será trabalhado o princípio da finalidade no capítulo 3. O referido princípio norteia as relações contratuais entre provedores e usuários na Internet. Assim sendo, os dados pessoais só podem ser coletados e utilizados para fins justificáveis, sendo vedado o uso indiscriminado destes.

Muitas dessas informações pessoais podem ser úteis em processos criminais, bem como investigações. Neste sentido, no capítulo 4 será abordada a cooperação destes provedores com as agências de segurança. A análise será feita através de um caso concreto, no qual o FBI - *Federal Bureau of Investigation* (Agência Federal de Investigação), órgão de inteligência da polícia dos Estados Unidos da América (EUA), requisitou o acesso à um celular para que procedesse, desta maneira, com a identificação de possíveis causas de um crime.

Por fim, para que se demonstre a interligação entre o princípio da finalidade, a coleta de dados, a fragilidade dos termos de uso e a cooperação com as agências de segurança, serão investigados os termos de uso de alguns provedores, são eles o *Pokémon Go*, o *Google* e o *Facebook*. Neste sentido, foi utilizado o método qualitativo para a análise dos referidos dados, sendo feita pesquisa bibliográfica e documental.

2 TERMOS DE USO

Os termos de uso são contratos eletrônicos feitos entre o Usuário e o Site, neles são previstas as condições às quais se está aderindo. Em se tratando de termos de uso, poucos são os usuários que os leem. Veja, por exemplo, que em 2005, o aplicativo PC Pitstop fez uma experiência e colocou no meio dos termos de uso uma cláusula que prometia uma bonificação ao primeiro usuário que enviasse um E-mail requisitando a recompensa. Levou mais de 5 meses e mais de 3 mil downloads para alguém requerer o prêmio (ROMERO, 2016).

Uma pesquisa feita pela Universidade de Stanford constatou que 97% dos usuários não leem os termos de uso (ROMERO, 2016). Em outra pesquisa, elaborada por Robert Hillman (apud LIMA, 2016), constatou que apenas 4% de seus alunos leem os contratos de adesão eletrônicos. Tais dados demonstram que o usuário não tem costume de ler o contrato eletrônico para a utilização do serviço.

O termo de adesão digital nada mais é que um contrato de adesão feito em meio virtual, tendo em vista que o usuário não tem o poder de negociar nenhuma das cláusulas ali inseridas. O conceito de contrato de adesão encontra-se no artigo 54 do Código de Defesa do Consumidor (BRASIL, 1990). Trata-se daquela avença na qual o consumidor não pode discutir ou modificar substancialmente seu conteúdo.

Há uma vantagem econômica para ambas as partes no contrato feito por adesão, pois conforme Robert Cooter e Thomas Ulen (2007), no contrato de adesão o risco e o preço são menores, pois não se barganha nada além do preço. Isso significa que o custo marginal do negócio é menor, até mesmo porque ante ao padrão de contratos, o fornecedor pode calcular melhor os riscos. Entretanto, do ponto de vista do consumidor, muitas das vezes em tais contratos são inseridas cláusulas limitativas de direitos, o que pode gerar nulidade, tendo em vista o disposto no Código Civil, conforme se verá adiante.

Pensando na proteção do consumidor a vista dessas cláusulas limitativas inseridas em contratos de adesão, o CDC normatiza que estas devem ser escritas com destaque, permitindo a fácil identificação, conforme o artigo 54, §4º (BRASIL, 1990). Mais ainda, tratando-se de contrato de adesão este deve ser escrito por inteiro em linguagem clara e de fácil compreensão, além da fonte ser de tamanho 12 no mínimo, conforme o §3º do mesmo dispositivo (BRASIL, 1990). Tais normas tem o fito de proteger o consumidor de práticas abusivas (TARTUCE, 2012). Entretanto, em alguns casos o usuário na internet sequer sabe da existência de um termo de uso que regula a relação. Isso decorre do fato de existirem dois tipos de contratos de adesão

eletrônico, os chamados Click-wrap e o Browse-wrap (LIMA, 2016). Wrap é uma palavra de origem inglesa, que significa embrulho. O intuito aqui é deixar claro que o contrato vem em um embrulho que deve ser clicado (Click-wrap) ou em um embrulho que é apenas navegado (Browse-wrap). Neste sentido, o contrato de Click-wrap é aquele por meio do qual o consumidor/usuário deve clicar na opção "Eu declaro que li e que concordo com os termos de uso e com a política de privacidade". Por sua vez, o contrato de Browse-wrap é aquele que regula a relação entre o provedor e o usuário, sem que ao menos este tenha manifestado a sua intenção através do clique (KLEE, 2012). É utilizada em sites em que não é necessário um cadastro prévio para uso, mas que utilizam cookies[3], por exemplo. É feita a coleta de dados do usuário, com a autorização do termo de uso, o qual não foi disponibilizado realmente ao usuário, quer seja através de uma pop-up[4] ou através de um aviso no próprio site, por exemplo.

Neste sentido, discute-se há vontade nestes contratos, elemento de todo contrato em uma visão clássica. Contrato que é a exteriorização de um negócio jurídico, sendo que "a exteriorização da vontade é a nota característica que mais avulta no negócio jurídica. É a sua força propulsora" (FARIAS; ROSENVALD, 2007, p. 428). Isso na concepção clássica, quando se falava em autonomia da vontade.

Entretanto, fala-se em crise contratual, com a mudança da autonomia da vontade, passando para a autonomia privada. Conforme Cesar Fiuza (2011) a autonomia da vontade remonta ao auge do liberalismo, momento em que se dava autonomia aos sujeitos, com a mínima intervenção estatal. Tal fato mudou com o avanço do capitalismo, o que fez com que acontece uma massificação dos contratos. Assim, os sujeitos não negociavam como antes, houve uma diminuição da vontade, que culminou na teoria preceptiva. Esta teoria ensina que "as obrigações oriundas dos contratos valem não apenas porque as partes as assumiram, mas porque interessa à sociedade a tutela da situação objetivamente gerada, por suas consequências econômicas e sociais" (FIUZA, 2011, p. 94). Conclui Cesar Fiuza (2011) afirmando que se passa de uma autonomia da vontade para uma autonomia privada, na qual não se tem na vontade uma lei máxima, que deve sempre prevalecer, podendo um contrato ser revisto caso se tenha um abuso de uma das partes, por exemplo.

No mesmo sentido:

[3] Cookies é uma forma de comunicação entre o site e o usuário. Trata-se do armazenamento das preferências do usuário naquele determinado site. O seu objetivo é aperfeiçoar a navegação, tendo em vista ser possível traçar um perfil pré-determinado dos gostos do usuário.

[4] Pop-up é uma janela que abre no navegador ao se clicar em um link específico, ou, até mesmo, acessar um website.

> É preciso aqui registrar, reiterando posição antes evidenciada à exaustão, que o elemento volitivo, fruto da autonomia da vontade e da autonomia privada, marca registrada do negócio jurídico, não mais assume caráter absoluto, sofrendo, sempre, as limitações decorrentes da ingerência de normas de ordem pública, notadamente constitucionais, por força da proteção destinada à pessoa humana, realçando sua necessária dignidade (art. 1º, III, CF/88). (FARIAS; ROSENVALD, 2007, p. 428)

Fala-se em crise contratual, tendo em vista a mudança de pensamento em relação ao elemento vontade. Há uma relativização dos seus efeitos. Conforme afirma Enzo Roppo (2009),

> Existe, sem dúvida, na evolução da teoria e da disciplina dos contratos, uma tendência para a progressiva redução do papel e da importância da vontade dos contraentes, entendida como momento psicológico da iniciativa contratual: esta tendência, que podemos definir como <objectivação do contrato>, leva a redimensionar, sensivelmente, a influência que o elemento voluntarista exerce, quer em relação à definição geral do próprio conceito de contrato, quer em relação ao tratamento jurídico concreto de cada relação (ROPPO, 2009, p. 297)

Portanto, o elemento vontade deixa de ser o preponderante em uma relação contratual, podendo se afirmar válido um contrato entabulado por adesão, ou seja, sem a discussão das cláusulas, pois nele há contato social, que segundo Roppo (2009) é o principal elemento jurígeno a formar o contrato. Neste sentido é que se posiciona pela validade dos termos de uso, o que não implica em afirmar que todas as cláusulas ali inseridas sejam válidas.

Em se tratando de Direitos da Personalidade, como o caso do direito a imagem, por exemplo, estes não podem sofrer uma limitação sem que isso seja expressamente concordado pelo usuário, com base no disposto no artigo 11[5] do Código Civil de 2002 (BRASIL, 2002). Ademais, existem diversas previsões de nulidades de cláusulas contratuais, tanto no CDC quanto no Marco Civil da Internet. Conforme normatiza o artigo 7º, inciso VI do Marco Civil, é assegurado ao usuário "informações claras e completas constantes dos contratos de prestação de serviços" (BRASIL, 2014). Trata-se, pois, de um dever do provedor de serviço informar ao usuário como é que será regida a relação, através dos termos de uso, dando possibilidade ao consumidor/usuário de conhecer as regras do serviço. Frisa-se que o artigo 8º do mesmo dispositivo normativo traz hipóteses de nulidades de cláusulas dos termos de uso. Veja-se:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

[5] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. (BRASIL, 2014)

Neste sentido, por mais que exista uma cláusula que implique nas hipóteses acima mencionadas, estas não terão validade. É uma forma de se tutelar o usuário ante aos termos de adesão, tendo em vista a falta de possibilidade de se escolher como vão ser tratados os dados pessoais, por exemplo.

Além do CDC e do Marco Civil, o Código Civil Brasileiro de 2002 possui duas normas que tratam do contrato de adesão, os artigos 423 e 424 (BRASIL, 2012). Tais normas tratam, respectivamente, do princípio da interpretação mais favorável ao aderente e da nulidade das cláusulas que tenham renúncia antecipada de direito. É uma proteção a mais para o usuário. Neste sentido, as cláusulas contratuais devem ser interpretadas de maneira mais favorável ao aderente, preservando, sempre que possível, a validade da avença.

Como os termos de uso dos serviços eletrônicos regulam aquela relação, nele são inseridas diversas condições para o uso, bem como das possibilidades de tratamento de dados pessoais, o que pode ferir a privacidade e intimidade do usuário. Surge a necessidade de se falar na finalidade do uso destes dados.

3 PRINCÍPIO DA FINALIDADE

O princípio da finalidade surge da preocupação com a coleta e tratamento de dados pessoais. Trata-se do princípio que determina que os dados pessoais devem ser utilizados com a finalidade para a qual foram coletados, impedindo a sua utilização para fins diversos do que o definido, ou seja, que haja tratamento secundário. Informa ainda esse princípio que o uso dos dados pessoais deve ser feito pelo tempo razoável que justifica sua coleta, passado isso, deve ser ele destruído.

Trata-se do princípio que decorre do próprio direito de privacidade, uma vez que, conforme Rodotá (2014), o direito de privacidade, na sociedade da informação, representa a possibilidade de seguir/controlar a própria informação onde quer que ela se encontre e se opor a qualquer interferência.

A preocupação com a coleta e tratamento de dados pessoais tem seu início com a inauguração do Estado Social conforme informa Mendes (2014). Assim é que o Estado passa a coletar a maior quantidade de informações possíveis de seus cidadãos de modo a efetivar políticas públicas assistencialistas. De fato, verificou-se que para cada benefício social

garantido, necessário se fazia a disponibilização de dados pessoais dos cidadãos, tais como, endereço, idade, gênero, estado civil, quantidade de filhos, renda, raça, entre outros. Desta feita, a partir da década de 70, quando os computadores começam a melhorar sua capacidade de processamento, passou-se a se preocupar com a possibilidade do Estado reunir em um único banco de dados as informações de seus cidadãos e dar tratamento diverso da finalidade para a qual foram coletados.

Conforme Mayer-Schoenberger (2001) a preocupação com a tutela dos dados pessoais nesse período não se tratava da garantia de um direito individual de privacidade, mas da tutela coletiva dos dados pessoais coletados, ou seja, tratava-se da necessidade de impor limites técnicos ao tratamento/coleta de dados pessoais.

A partir da década de oitenta com a difusão da internet, a preocupação passa a ser com a possibilidade de cruzamento de dados entre os diferentes bancos de dados, ou seja, a tutela dos dados pessoais não se refere apenas a impor limites técnicos à criação de um único banco de dados nacional a poder do Estado, mas, sobretudo a possibilidade de tratamento desses dados e a comunicação entre os diversos bancos de dados, sejam públicos ou privados. Segundo Mendes (2014), passa-se a reivindicar o direito da autodeterminação informativa, ou seja, a possibilidade de a pessoa controlar o processamento de seus dados pessoais, ou seja, a coleta/transmissão/armazenamento de seus dados pessoais.

Essas informações podem ser confirmadas pelo emblemático caso julgado pelo Tribunal Constitucional alemão de 1983 sobre a lei do senso (SCHWABE, 2005). O Governo alemão ao editar uma lei sobre recenseamento de sua população permitiu que os dados coletados com a finalidade de recenseamento pudessem ser aproveitados para outras finalidades. Assim é que o Tribunal Constitucional declarou a impossibilidade de aproveitamento desses dados para finalidades diversas do recenseamento.

Atualmente a preocupação com a tutela dos dados pessoais ganha novos contornos, na medida que o fornecimento de dados pessoais se intensifica com a inauguração das redes sociais, bem como a difusão de aplicativos para *smartphones*. As informações extraídas dos dados pessoais passam a ser a moeda valiosa para os provedores de serviços de internet. Informações estas que são requeridas por esses provedores e retroalimentadas pelos próprios usuários em um fluxo constante. Assim é que ao se utilizar pela primeira vez um serviço de aplicação de internet é solicitado ao usuário o fornecimento de alguns dados pessoais e que serão constantemente coletados enquanto do uso desse serviço, como por exemplo os registros de localização, entre outros.

Nessa medida autores como Cate, Cullen e Mayer-schoenberger (2013) destacam a necessidade da releitura dos princípios que garantem a proteção dos dados pessoais e em especial o princípio da finalidade. Desta feita a coleta/tratamento de dados pessoais não pode ser feita através de engano, de maneira não explícita ou não perceptível ao usuário. Ainda, o uso/tratamento dos dados pessoais deve sofrer limitações em razão dos riscos de dano ao titular do dado pessoal, desta feita, quanto maior a possibilidade dano ao usuário, menor será a possibilidade de tratamento/utilização desse dado. Ademais, a utilização de dados pessoais sempre apresenta um risco, devendo sua utilização estar, também, limitada em conformidade com a proteção a danos que podem surgir desse tratamento. Assim é que esses autores simplificam que na utilização/tratamento de dados pessoais se deve trabalhar com os vetores dos riscos e benefícios que esse tratamento pode oferecer, devendo haver um equilíbrio entre eles.

A ONU (Organização das Nações Unidas), em 2011, definiu os princípios e direitos que informam a governança digital, são eles: Universalidade e igualdade; Direito e Justiça Social; Acessibilidade; Expressão e Associação; Privacidade e Proteção de Dados; a Vida, Liberdade e Segurança; Diversidade; Rede de Igualdades; Padrões e Regulamentos; e Governança (IGF, 2016).

Desta feita a proteção de dados pessoais é um princípio fundamental da internet e deve ser perseguida pelos Estados.

No Brasil, assim como se pode observar nos demais Estados, a proteção de dados pessoais não se resume ao princípio da finalidade, mas por uma questão de corte científico, nesse artigo, trabalhar-se-á de modo principal com o princípio da finalidade.

No marco civil da internet (Lei 12.965/2014) o princípio da finalidade pode ser extraído do artigo 7º, VII, VIII e IX, bem como no artigo 13, §2º do regulamento do marco civil da internet (Decreto nº8771/2016).

Determina o artigo 7º do marco civil (BRASIL, 2014) que é direito do usuário da internet, entre outros: o não fornecimento de seus dados pessoais salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; o consentimento expresso sobre o uso/armazenamento/tratamento dos dados pessoais deverá ocorrer de forma destacada das demais cláusulas contratuais; ter informações claras e completas sobre o uso/armazenamento/tratamento de seus dados pessoais; ainda que o uso/armazenamento/tratamento dos dados pessoais deverão atender as finalidades que

justifiquem a sua coleta, que não sejam vedadas pela legislação e que estejam especificadas nos termos de uso de serviço.

Conforme o regulamento do marco civil (BRASIL, 2016) os provedores devem reter a menor quantidade possível de dados pessoais, devendo os mesmos serem excluídos tão logo seja atingida a finalidade do seu uso ou ter se encerrado o prazo determinado por obrigação legal, que conforme o marco civil os provedores são obrigados a armazenarem os registros de acesso pelo prazo de 6 (seis) meses – artigo 15 do marco civil da internet. O regulamento, em seu artigo 14, define como dado pessoal o dado relacionado "à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016) e como tratamento de dados pessoais:

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2016)

Está claro, portanto, que a legislação brasileira reconhece o princípio da finalidade, determinando que a utilização dos dados pessoais deve observar a finalidade para a qual foi feita essa coleta, devendo ser oportunizado ao usuário o conhecimento sobre a uso/armazenamento/tratamento desses dados de forma destacada, e clara, mediante consentimento informado, livre e expresso.

4 DA COOPERAÇÃO COM AGÊNCIAS DE SEGURANÇA

Uma preocupação que se tem em se tratando de dados pessoais na era digital é com o uso destes. Em grande maioria, os termos de uso dos serviços utilizados não deixam claro se há o compartilhamento destes com agências de seguranças. Conforme relatório do Google, apenas neste serviço durante o período de julho a dezembro de 2015, foram feitas mais de 40 mil solicitações por 101 países, sendo atendidas 64%. No Brasil, foram feitas 912 solicitações, sendo atendidas 57% destas, com a especificação de 2.041 usuários (GOOGLE, 2016a). Isso demonstra que é preciso que se discuta a forma como esses dados são passados à essas agências.

Um recente caso envolvendo a Apple e o FBI demonstra a fragilidade da cooperação entre empresas privadas e agências de segurança. Trata-se de uma solicitação feita pelo FBI à Apple requerendo que fosse criado um código mestre para acesso ao IPhone de um criminoso.

O argumento utilizado pelo FBI foi de que com a investigação do conteúdo do IPhone seria possível descobrir as causas e os demais envolvidos no delito. Por sua vez, a Apple argumentou que a criação de um código único poderia pôr em risco a privacidade dos demais usuários, negando, pois, a solicitação feita pelo FBI (CHAMY, 2016).

Instaurou-se uma série de debates sobre o caso, sendo que o FBI insistia no argumento de que a segurança da coletividade se sobrepunha ao direito de privacidade dos usuários. Ao fim, a Apple não cedeu as exigências da Agência, mas o FBI conseguiu acesso ao conteúdo do telefone através de terceiros (hackers), que conseguiram quebrar o código de segurança daquele dispositivo (FBI, 2016).

Evidente que a cooperação com as agências de inteligência dos Estados Unidos decorre de lei daquele país. Trata-se da aplicação da Lei de Vigilância de Inteligência Estrangeira (FISA) datada de 1978 a qual regulamenta como é a coleta de dados pessoais por Agências de Inteligência (FOREIGN, 2016). A referida lei criou o Tribunal de Vigilância de Inteligência Estrangeira (FISC), o qual analisa os pedidos de coleta de dados pessoais.

Ademais, existe nos EUA a Lei de Privacidade das Comunicações Eletrônicas (EPCA) (ELECTRONIC, 2016). A referida lei estabelece o procedimento para o FBI realizar interceptação de dados em caso de investigações. Com base nesta lei, é possível que o FBI solicite a qualquer provedor informações que "identifiquem uma pessoa, entidade, número de telefone, ou conta como base para um pedido"[6] (tradução nossa, COUNTERINTELLIGENCE, 2016).

Evidente que existe um princípio de cooperação entre as empresas privadas e as Agências de Inteligência. Isso se mostra necessário face à necessidade de segurança para toda a população, tendo em vista que através da cooperação destas empresas com o fornecimento de dados pessoais dos usuários, as agências de segurança podem agir de forma eficaz no combate de condutas delituosas. Entretanto, é preciso que essa cessão de dados pessoais não se caracterize como uma espionagem, como denunciado por Edward Snowden. Ficou provado que o serviço de inteligência americana monitorava os E-mails dos governantes de diversos países, entre eles o Brasil (BRANT, 2014).

Em junho de 2013, o The Guardian publicou uma reportagem que apontava aquilo que Edward Snowden havia denunciado (GREENWALD, 2016). Snowden foi agente de segurança da Agência de Segurança Nacional (NSA) dos EUA, momento em que constatou que mais do

[6] Original: identifies a person, entity, telephone number, or account as the basis for a request.

que requisitar informações sobre usuários em uma investigação, a referida agência monitorava constantemente os usuários.

Até mesmo dados de usuários brasileiros foram monitorados, inclusive de agentes diplomáticos e de pessoas ligadas à presidência (GREENWALD; KAZ; CASADO, 2016). Isso demonstra a fragilidade da possibilidade de uma intercepção por motivos de segurança. Não se quer dizer que não deve existir uma cooperação entre provedores e agências de segurança, tendo em vista a necessidade de se tutelar a segurança coletiva. Afirma-se na legitimidade em requisitar dados pessoais, desde que necessário à uma investigação já em curso. Até mesmo porque, caso se tenha um monitoramento constante, todos os usuários serão penalizados com a perda da intimidade e privacidade.

O Marco Civil da Internet aprovado em 23 de abril de 2014, durante o evento denominado de NETmundial na cidade de São Paulo, teve em seu contexto de criação discussões que remontavam às investigações feitas pelo serviço de inteligência dos Estados Unidos, denunciado por Edward Snowden no ano de 2013 (BRANT, 2014), o que foi tratado como um escândalo mundial. Assim, a então presidente, ao realizar o discurso de abertura da 68ª Assembleia-Geral das Nações Unidas no dia 24 de setembro de 2013, afirmou que:

> Recentes revelações sobre as atividades de uma rede global de espionagem eletrônica provocaram indignação e repúdio em amplos setores da opinião pública mundial.
> No Brasil, a situação foi ainda mais grave, pois aparecemos como alvo dessa intrusão. Dados pessoais de cidadãos foram indiscriminadamente objeto de interceptação. Informações empresariais – muitas vezes, de alto valor econômico e mesmo estratégico - estiveram na mira da espionagem.
> [...]
> Sem ele – direito à privacidade - não há verdadeira liberdade de expressão e opinião e, portanto, não há efetiva democracia
> [...]
> Por essa razão, o Brasil apresentará propostas para o estabelecimento de um marco civil multilateral para a governança e uso da internet e de medidas que garantam uma efetiva proteção dos dados que por ela trafegam. (ROUSSEFF, 2016).

A partir desse momento acelerou-se a elaboração do projeto de lei, para que ele fosse lançado no NETmundial, evento internacional de tecnologia que aconteceria em São Paulo no ano seguinte.

Referida Lei possui uma disposição sobre a cessão de dados pessoais por parte dos entes privados. Entretanto, é necessário um requerimento judicial para que se tenha a disponibilidade dos dados pessoais, conforme artigo 22 do Marco Civil. Veja-se:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao

> juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros. (BRASIL, 2014)

Mais ainda, o artigo 7º do Marco Civil, nos incisos I, II e III (BRASIL, 2014) normatiza a inviolabilidade das comunicações feitas pela Internet, resguardando sempre a intimidade e privacidade dos usuários, o que é um dos pilares da Lei.

Isso demonstra a preocupação em se tutelar os direitos e garantias individuais, o que não importa afirmar que não é possível ter acesso às comunicações privadas. Isso porque, ao contrário do sistema norte-americano, o sistema brasileiro exige a efetiva atuação do Poder Judiciário, não autorizando a interceptação de quaisquer dados sem a efetiva prestação jurisdicional. Entretanto, como a maioria dos serviços da Internet possuem sede no Vale do Silício que se localiza nos EUA, estes são obrigados a cumprir as exigências feitas por aquela legislação, o que faz com que a maioria dos serviços coloquem cláusula que possibilita a cooperação nos termos de uso, o que não é feito de forma expressa em muitos dos casos. Entre os mais utilizados estão o *Facebook* e o *Google*. Caso recente que gerou uma preocupação dos usuários foi o jogo *PokémonGo*.

5 ANÁLISE DOS TERMOS DE USO EM RELAÇÃO AO USO/ARMAZENAMENTO/TRATAMENTO DE DADOS PESSOAIS

De modo a ilustrar o trabalho será feita a análise de como alguns aplicadores de serviço de internet, em seus termos de uso, especificam como se dará o uso/armazenamento/tratamento dos dados pessoais, bem como a possibilidade ou não de cooperação com agências de segurança. Forma eleitos os serviços do *Pokémon Go*, do *Google* e do *Facebook*.

A *Niantic*, desenvolvedora do jogo *Pokémon Go*, em seu termo de uso do serviço[7] (NIANTIC, 2016) informa que ao aderi-lo o usuário também concorda com sua política de privacidade. Informa sobre a impossibilidade de alteração de qualquer cláusula contratual por parte do aderente e que caso haja a discordância com as mesmas, recomenda que não seja utilizado o serviço. Informa ainda que crianças menores de 13 anos poderão utilizar o serviço,

[7] Para esse trabalho foi consultada a versão de 1 de julho de 2016, última atualização disponibilizada pelo desenvolvedor do jogo.

mas a aceitação dos termos se dará na figura dos pais ou representante legal, ou seja, que essas pessoas aceitarão os termos de uso por elas mesma e pelo incapaz.

Informa ainda que poderá ser feita alterações a qualquer tempo nos termos de uso e política de privacidade que serão comunicadas através do aplicativo, site oficial ou outro meio. Caso o usuário não concorde com as alterações o serviço poderá ser descontinuado, ou seja, para continuar usando o aplicativo deve-se concordar com as alterações apresentadas.

De forma destacada informa que, na exceção de ter aceitado os termos por *Opt-Out* ou em alguns casos previstos no acordo de arbitragem que compõe o termo de uso, o usuário renuncia ao direito de propor demanda judicial e concorda com a cláusula arbitral. Informa que a legislação aplicável para solucionar conflitos é a lei da Califórnia. Esse tipo de cláusula é controversa no ordenamento jurídico brasileiro, pois tem-se considerado que a cláusula arbitral em contratos de adesão em relação de consumo não podem ser impostas ao consumidor. Só terão eficácia se o consumidor ratificar após a sua instituição ou se o próprio consumidor tomar a iniciativa no exercício da cláusula arbitral[8]. Ainda no que se refere ao conflito de leis no espaço, a escolha da lei aplicável por autonomia privada só é possível nos casos em que não haja competência exclusiva da lei brasileira. A doutrina vem entendo que em relações de consumo, por ser a Lei 8078/90 uma norma de ordem pública, tem aplicação direta e imediata, e segundo Cláudia Lima Marques (2011), não poderá ser afastada, a menos que a lei estrangeira seja mais favorável ao consumidor.

Em sua política de privacidade, a Niantic (2016) informa que o principal objetivo na coleta de dados pessoais é oferecer o próprio serviço e melhorá-lo. Informa que durante o uso do jogo serão coletados dados, como nome e mensagens enviadas a outros usuários. Contudo, esclarece que esses dados não permitirão que terceiros identifiquem o usuário, a menos que o próprio usuário informe seu nome verdadeiro ou outros dados que possam o identificar. Informa, ainda, que utiliza *cookies*[9] e *web beacons* ou etiqueta *pixel*[10] com a finalidade de melhorar o serviço prestado. Em relação aos *cookies* são coletadas informações de quando o

[8] É o que se pode extrair do REsp 1.189.050 (BRASIL, 2013)

[9] "O cookie é um arquivo de texto que tem como principal função armazenar as preferências do usuário em todos os sites. Quando você busca algum produto em determinado site e ele aparece em sua tela quando você navega em outras páginas, foi o cookie quem informou isso ao sistema. É o cookie quem diz que você é você e que você queria aquele produto". (PRIVACIDADE NA INTERNET, 2016)

[10] "Os web beacons podem estar presentes em páginas da web ou mesmo em e-mails. Eles permitem, quando o usuário clica em imagens, que um site consiga coletar ou transferir informações para o usuário. Com os web bugs, assim também chamados, o seu computador pode ser monitorado de forma que seja possível verificar seus e-mails, os seus dados armazenados na máquina. Se um remetente lhe envia um web beacon mascarado, ele pode conseguir ter acesso a seu e-mail e utilizá-lo para enviar diversos spams para demais usuários". (PRIVACIDADE NA INTERNET, 2016)

aplicativo é acessado e para informar quando e como o usuário interagiu com alguns dos serviços do aplicativo. Informa que os *cookies* de sessão serão excluídos quando o usuário sair do serviço e encerrar o navegador, mas que permaneceram os *cookies* persistentes que irão identificar como o usuário utiliza o serviço ao longo do tempo. Caso o usuário opte por restringir o uso de *cookies* no navegador, impedindo de recebê-los de forma automática, o usuário possivelmente não conseguirá ter acesso a todas as funções do aplicativo. Informa que terceiros contratados pelo provedor poderão colocar *cookies* no disco rígido do usuário. Os *web beacons* são utilizados para interagir com os *cookies*, melhorar o desempenho do aplicativo, monitorar a quantidade de visitantes, monitorar a eficácia da publicidade, entre outras possibilidades.

O Compartilhamento de dados com terceiro não é de uso livre pelo provedor, a *Niantic* (2016) estipula os termos nos quais poderá haver esse compartilhamento. Informa que poderá haver o compartilhamento de dados identificáveis com a *The Pokémon Company* e com *The Pokémon Company International*[11] caso o usuário tenha uma conta nessas companhias e exista algum erro que só possa ser solucionado com a colaboração das mesmas. A *Niantic* pode contratar terceiros prestadores de serviços para administrar e prover o seu serviço, caso em que terão acesso a dados identificáveis. Mas alerta que esses terceiros não poderão utilizar esses dados com finalidade diversa da prestação de serviço contratada e deverão manter esses dados seguros.

Poderá haver o compartilhamento de dados não identificáveis com terceiros ou de dados agregados com a finalidade de pesquisa, análise e identificação de perfil demográfico e outros fins semelhantes.

Informa ainda (NIANTIC, 2016) que os dados pessoais, identificáveis ou não são um ativo comercial e terão valor em uma possível alienação, caso em que esses dados poderão ser cedidos a um terceiro. Nesse caso a *Niantic* dará ao usuário a opção de recusar a divulgação ou transferência dos dados pessoais ao terceiro comprador em um prazo de 30 dias.

A *Niantic* informa (NIANTIC, 2016) que coopera com autoridades do governo e entidades privadas para aplicação e cumprimento da lei. Dessa forma pode divulgar quaisquer dados sobre o usuário que esteja sobre seu controle às autoridades governamentais de modo a

[11] A criação de contas nesses provedores se torna obrigatória se o usuário for uma criança menor de 13 anos. Caso em que os pais ou responsáveis deverão registrar no Clube de treinadores Pokémon que irá direcionar para o site do The Pokémon Company International de modo a confirmar dados que informe ser o representante legal do menor e que concorda com as políticas de privacidade, permitindo o incapaz a utilizar o serviço. Nos demais casos para utilizar o app, o usuário pode ter uma conta no Google, Facebook ou no clube de treinadores Pokémon (NIANTIC, 2016).

responder a ordens judiciais; proteger seus próprios bens, direitos e segurança, bem como bens, direitos e segurança de terceiros ou de toda a sociedade; e para interromper qualquer atividade considerada por ela como ilegal e antiética. Como se pode depreender não está expressa a cláusula de cooperação com agências de segurança, apenas é informado que serão transmitidos dados identificáveis quando a lei ou o judiciário o determinar, bem como em casos de segurança do próprio desenvolvedor, de terceiros ou da sociedade, sempre através de seu próprio crivo. A cláusula não pode ser considerada inválida no ordenamento jurídico brasileiro e acaba por permitir esse tipo de cooperação ao crivo do provedor conforme informado em sua política de privacidade. Já se demonstrou nesse artigo que o marco civil da internet no artigo 7º inciso VII permite o fornecimento de dados a terceiros desde que haja consentimento livre, expresso e informado. Talvez a grande dificuldade seja estabelecer o que seja consentimento informado. Como já se trabalhou, os termos de uso/políticas de privacidade são contratos de adesão e, conforme demonstrado em pesquisas, os consumidores não leem seus termos. Assim é que a informação está disponível ao usuário, mas seu consentimento está mesmo informado? Aqui se encontra, possivelmente, um dos maiores desafios do Direito Digital no que concerne a proteção de dados pessoais.

A *Google* (GOOGLE, 2016b) em sua política de privacidade[12] não apresenta disposições muito diferentes da *Niantic*. Informa que a coleta de dados tem a finalidade de melhorar os serviços prestados a seus usuários. Informa que pode analisar os mesmos para descobrir idiomas, preferências dos usuários, identificar pessoas que são mais importantes para os usuários, entre outras informações. Informa que coleta os dados que os usuários transmitem de forma direta, por exemplo, os dados que são requeridos quando da criação da conta *Google* (nome, e-mail, número de telefone, cartão de crédito). Mas que também coleta dados a partir do uso que o usuário faz de seus serviços, por exemplo como e quando usa e quais serviços são utilizados, como interage com anúncios e conteúdos disponibilizados. Informa que coleta e processa dados sobre a localização real do usuário, seja através de dispositivo de GPS, IP, ou outros sensores que podem permitir a *Google* a coleta de dados dos dispositivos, tais como pontos de acesso de *wi-fi* e torres de celulares próximos. É interessante ressaltar que uma das maiores preocupações que se teve com o aplicativo do *Pokémon Go* foi justamente o uso de localizadores que a *Google* já utilizava a mais tempo.

A *Google* (GOOGLE, 2016b) informa utilizar a tecnologia de *cookies* e *web beacons*. Contudo ressalta que quando exibe anúncios personalizados, que são baseados nessas

[12] A versão utilizada para a realização de artigo é de 29 de agosto de 2016.

tecnologias, não associa identificadores provenientes de dados sensíveis, tais como raça, religião, orientação sexual ou saúde. Informa ainda que a utilização de dados pessoais com finalidade diversas das estipuladas em sua política de privacidade deverá ser autorizada pelo usuário. Cabe ressaltar que a *Google* oferece uma série de opções a seus usuários de modo a controlar suas atividades nos serviços *Google*, podendo rever, controlar, ajustar como serão utilizados seus dados pessoais.

A *Google* informa (GOOGLE, 2016b) que não compartilha informações pessoais com empresas, organizações e indivíduos externos à *Google*, salvo nas hipóteses previstas em sua política de privacidade. Assim é que poderá ser compartilhadas essas informações se houver autorização do usuário e em caso de dados sensíveis, considerada pela *Google* como "informações pessoais confidenciais relacionadas a dados médicos, origens raciais ou étnicas, crenças religiosas, políticas ou sexualidade"(GOOGLE, 2016c), essa autorização deverá ser colhida pelo sistema de *opt-in*. Também serão compartilhadas as informações com prestadores de serviços ao *Google* para processamento dessas informações em conformidade com a política de privacidade da *Google*. Essas informações poderão ser compartilhadas, a critério da *Google*, com empresas, organizações e indivíduos externos à *Google* por motivos legais. São casos em que dever-se-á cumprir legislação, regulamento, ordem judicial ou governamental; para que se cumpra termos de serviços aplicáveis ou a investigação de sua violação; por questões de segurança ou técnicas para impedir fraudes; em caso de danos a bens ou direitos da *Google*, de seus usuários ou da coletividade conforme solicitado ou permitido por lei.

Observe que a *Google*, assim como a *Niantic* não informam de modo explícito a cooperação com agencias de segurança. Mas isso pode acontecer desde que haja ordem judicial, determinação legal ou quando, a critério da *Google*, se considerar a possibilidade de segurança de outros usuários, dela própria ou da sociedade em geral.

As informações não identificáveis, segundo a *Google* (GOOGLE, 2106b), podem ser livremente compartilhadas com terceiros e, em havendo alienação, a divulgação de dados identificáveis ao terceiro comprador só se dará após a autorização do usuário.

O *Facebook* (FACEBOOK, 2016) apresenta política de privacidade semelhante às já explicadas aqui. Em relação ao fornecimento de dados pessoais a terceiros informa de modo claro que compartilha os mesmos com parceiros e clientes terceiros. Assim como os demais casos já aqui analisados, informa que pode terceirizar a execução dos seus serviços, caso em que essas empresas terão acesso aos dados pessoais de seus usuários. Informa que compartilha dados não identificáveis para serviços de publicidade, mediação e análise.

Assim como a *Google* e a *Niantic*, o *Facebook* responde a solicitações judiciais e a legislação. Desta forma, pode transmitir a terceiros dados pessoais identificáveis. Informa ainda que em casos de fraude, segurança do próprio *Facebook*, de seus usuários ou da coletividade, pode fornecer dados, inclusive para fins de investigação criminal, governamental ou até mesmo para fins de prevenção de violação de sua própria política de privacidade.

6 CONCLUSÃO

Observa-se que na sociedade da informação com o uso aumentado dos dados pessoais e o tratamento dos mesmos, há que se refletir sobe a finalidade de sua coleta, bem como se os provedores de aplicações de internet serão obrigados a cooperar com agências de inteligência.

Viu-se que o tratamento dos dados pessoais pelos provedores de aplicação de internet é regulado por termos de uso/políticas de privacidade que possuem natureza jurídica de contrato de adesão. Desta feita, explicou-se o que venha a ser contrato de adesão. Conclui-se neste ponto que os contratos de adesão alteram a forma clássica de contrato que via a vontade como o elemento jurígeno principal na formação do mesmo. Conforme foi explicitado o contrato é formado pelo contato social. Ainda, pelo fato de sua natureza de adesão esses contratos recebem do ordenamento jurídico uma forma de interpretação mais protetiva aquele que adere. Assim é que o Código de Defesa do Consumidor, o Código Civil, bem como o Marco Civil, legislações estudadas nesse artigo, apresentam regras para cláusulas limitativas de direitos dos aderentes. Desta feita, há que se terem cláusulas claras, destacadas sobre o tratamento de dados dos usuários de aplicações de internet, bem como a colhida livre, bem informada e inequívoca para o tratamento desses dados.

Assim que é outro ponto importante demonstrado no artigo é o princípio da finalidade, presente tanto em diretriz da ONU, bem como no marco civil da internet. Assim, os provedores de aplicações de internet, ao fazer uso/tratamento de dados pessoais de seus usuários devem atender a finalidade para a qual a coleta se deu. E quando o uso se der para outra finalidade, tal como a possibilidade de cooperação com agências de inteligências, isso deve estar de forma clara, bem informada e com autorização do usuário. Observe que, conforme explicitado, sem a autorização do usuário, o provedor está obrigado, segundo a regras do marco civil da internet, a fornecer esses dados quando houver requisição judicial.

Nessa pesquisa, ficou ainda evidenciado que nos EUA os provedores de aplicações de internet estão obrigados a cooperarem com agências de inteligência, por determinação da Lei

de Vigilância de Inteligência Estrangeira. Ainda, que os provedores de aplicações estudados neste artigo estão sitiados nos EUA, devendo respeitar essa lei. Contudo, no Brasil, estão adstritas as leis brasileiras e devem respeitar o marco civil que determina que a cessão de dados de seus usuários deve ser feita quando houver determinação judicial para tanto, ou para a finalidade pela qual estão determinadas em seus termos de uso/política de privacidade.

Por fim, da análise dos termos de uso/política de privacidade dos provedores de aplicações de serviços de internet utilizadas nessa pesquisa, viu-se que nenhuma delas estipula de maneira clara sobre a cooperação com agência de inteligência. Contudo explicitam e de forma destacada, que a seu critério, em um juízo de boa-fé, poderão ceder os dados coletados todas as vezes que houver a possibilidade de violação da segurança de outros usuários, dos próprios provedores ou da sociedade em geral.

REFERÊNCIAS

BRANT, Cássio Augusto Barros. **Marco Civil da Internet: comentários sobre a Lei 12.965/2014**. Belo Horizonte: Editora D'Plácido, 2014.

BRASIL, Superior Tribunal de Justiça. RECURSO ESPECIAL Nº 1.189.050 – SP. Rel. MINISTRO LUIS FELIPE SALOMÃO. **Diário da Justiça**, Brasília 14 out. 2013.

BRASIL. DECRETO Nº 8.771 DE 11 DE MAIO DE 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. **Diário Oficial da União**. Brasília, 11 maio. 2016.

BRASIL. LEI Nº 10.406, DE 10 DE JANEIRO DE 2002. Institui o Código Civil. **Diário Oficial da União**. Brasília, 11 Jan. 2002.

BRASIL. LEI Nº 12.965, DE 23 ABRIL DE 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**. Brasília, 24 ABR. 2014.

BRASIL. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**. Brasília, 12 Set. 1990.

CATE, Fred H. CULLEN, Peter. MAYER-SCHÖNBERGER,Viktor. **Data Protection Principles for the 21st Century**: Revising the 1980 OECD Guidelines. Microsoft Corporation, 2013.

CHAMY, Constanza Hola. **Como o FBI conseguiu desbloquear o iPhone de suspeito de ataque à revelia da Apple?.** BBC. Disponível em <http://www.bbc.com/portuguese/noticias/2016/03/160330_fbi_apple_lab >. Acesso em 22 ago. 2016

COUNTERINTELLIGENCE access to telephone toll and transactional records. Cornell University. Disponível em <https://www.law.cornell.edu/uscode/text/18/2709 >. Acesso em 22 ago. 2016

ELECTRONIC Communications Privacy Act of 1986 (ECPA). Justice Information Sharing. Disponível em < https://it.ojp.gov/privacyliberty/authorities/statutes/1285>. Acesso em 22 ago. 2016

FACEBOOK. Política de dados. Disponível em <https://www.facebook.com/privacy/explanation> acesso em 19 de ago. 2016.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Direito Civil: Teoria Geral.** 6ª ed. Rio de Janeiro: Lumen Juris, 2007

FBI pagou hackers para acessar iPhone de atirador, diz jornal. G1. Disponível em <http://g1.globo.com/tecnologia/noticia/2016/04/fbi-pagou-hackers-para-acessar-iphone-de-atirador-diz-jornal.html>. Acesso em 22 ago. 2016

FIUZA, César. **Direito Civil: Curso Completo.** 15ª ed. Belo Horizonte: Del Rey, 2011

FOREIGN Intelligence Surveillance. Cornell University. Disponível em < https://www.law.cornell.edu/uscode/text/50/chapter-36>. Acesso em 22 ago. 2016

GOOGLE. **Google Privacidade & Termos**. Disponível em <https:// www.google.com.br/policies/privacy//> acesso em 19 de ago. 2016b

GOOGLE. **Google Transparency Report.** Disponível em <https://www.google.com/transparencyreport/userdatarequests/countries/> acesso em 19 de ago. 2016a

GOOGLE. **Termos-chave**. Disponível em < https://www.google.com/intl/pt-BR/policies/privacy/key-terms/#toc-terms-sensitive-info> acesso em 19 de ago. 2016c

GREENWALD, Glenn. **NSA collecting phone records of millions of Verizon customers daily.** The Guardian. Disponível em < https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. Acesso em 22 ago. 2016

GREENWALD, Lenn; KAZ, Roberto; e CASADO, José. **EUA espionaram milhões de e-mails e ligações de brasileiros.** O Globo. Disponível em < http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em 22 ago. 2016

IGF, Internet Governace Forum. **Carta de Direitos Humanos e Princípios para a Internet**. Out, 2015. Disponível em <http:// Carta de Direitos Humanos e Princípios para a Internet>, acesso em 18 de ago. 2016.

KLEE, Antonia Espíndola Longoni. **O diálogo das fontes nos contratos pela internet: do vínculo contratual ao conceito de estabelecimento empresariam virtual e a proteção do consumidor**. In: MARQUES, Claudia Lima. Diálogo das Fontes: Do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012. p. 399/450.

LIMA, Cíntia Rosa Pereira De. **O Ônus de Ler o Contrato no Contexto da "Ditadura" dos Contratos de Adesão Eletrônicos**. Disponível em < http://publicadireito.com.br/artigos/?cod=981322808aba8a03>, acesso em 18 ago. 2016

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais.** 6 ed. Ver., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2011

MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. In: AGRE, Philip E.; ROTENBERG, Marc. Technology and privacy: the new landscape. Cambridge: Mit, 2001.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor linhas gerais de um novo direito fundamental**. São Paulo Saraiva 2014

NIANTIC. **Política de privacidade Pokémon GO**. Versão de 1 de julho de 2016. Disponível em < https://www.nianticlabs.com/privacy/pokemongo/en> acesso em 19 de ago. 2016

PRIVACIDADE NA INTERNET. **UOL, Postado em 29/08/2013**. Disponível em <http://seguranca.uol.com.br/antivirus/dicas/curiosidades/privacidade-na-internet-conheca-os-cookies-web-beacons-e-flash-cookies.html#rmcl> acesso em 19 de ago. 2016.

RODOTÁ, Stefano. **Il mondo nella rete: quali i diritti, quali i vincoli**. Roma: Laterza, 2014.

ROMERO, Luiz. **Não li e concordo.** Super Interessante. Disponível em <http://super.abril.com.br/tecnologia/nao-li-e-concordo>. Acesso em 22 ago. 2016

ROPPO, Enzo. **O Contrato**. Coimbra: Almedina, 2009

ROUSSEFF, Dilma. **Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas - Nova Iorque/EUA.** Disponível em: http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua. Acesso em 10 jul. 2016

SCHWABE, Jürgen. MARTINS, Leonardo (Org.). HENNIG, Beatriz e Outros (trad.). **Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Berlin: Konrad-Adenauer-Stiftung, 2005.

TARTUCE, Flávio. **A teoria geral dos contratos de adesão no Código Civil. Visão a partir da teoria do diálogo das fontes**. In: MARQUES, Claudia Lima. Diálogo das Fontes: Do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012. p. 205/232.