PRIVACIDADE EM TEMPOS DE INTERNET: UMA APRECIAÇÃO DA DIMENSÃO ECONÔMICA NO TRATAMENTO DE DADOS PESSOAIS

Bernardo Felipe Estellita Lins
Consultor Legislativo da Área XIV
Ciência e tecnologia, Comunicação Social, Informática, Telecomunicações e Sistema Postal

ESTUDO TÉCNICO

JANEIRO DE 2018

SUMÁRIO

Resumo

A evolução da internet vem impondo mudanças de hábitos, práticas e valores que permeiam as várias relações sociais. Um aspecto que vem passando por importantes transformações é o da privacidade, podendo resultar em novas interpretações do modo como sua garantia constitucional deva ser aplicada. Além da Constituição, o texto usa os dispositivos do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) como guia para abordar aspectos que vêm sendo evidenciados pelo debate dos problemas de privacidade que emergem do uso da rede mundial.

Palavras-chave: economia da internet, guarda de registros, privacidade, responsabilidade por danos a terceiros

INTRODUÇÃO

O surgimento da internet comercial no início dos anos noventa (e sua operação no Brasil a partir de 1994) deu início a uma transformação em grande escala na organização da sociedade brasileira. Há vários textos descritivos de como essa evolução social vem se processando e de várias de suas implicações para o tecido econômico, o comportamento das pessoas, seus hábitos de consumo e o modo como se dão as relações sociais e o debate público (BOYD e ELLISON, 2008; LINS, 2013; TIGRE, 2014; SCHWAB, 2016).

Do ponto de vista do tratamento da norma constitucional, há implicações importantes a considerar. Em parte, a Constituição reflete valores fundamentais da sociedade e suas convicções morais e políticas, tendo nesse sentido um caráter universal e imutável. Também incorpora, por outro lado, aspectos de um contrato social que é permanentemente questionado e negociado, necessitando de atualizações para acompanhar os elementos legítimos desse reposicionamento dos acordos que são construídos. Se assim não ocorresse, a Carta se tornaria inaplicável à realidade social que pretende balizar.

Essa evolução pode ser construída de diversas formas, alcançando a recodificação de dispositivos da norma constitucional, a mudança de orientação na sua hermenêutica e a construção de uma jurisprudência decorrente da sua aplicação ao exame de dispositivos infraconstitucionais ou até diretamente a casos concretos. No Brasil, vivemos na última década um ambiente que reflete esse reposicionamento, seja pela abundância de emendas à Constituição, que já somam quase uma centena nos trinta anos de vigência da Carta, sendo mais de quarenta nos últimos dez anos, seja pela crescente elasticidade na interpretação dos comandos constitucionais pelo Supremo Tribunal Federal, resvalando por vezes em um clima de insegurança jurídica.

Diante desse contexto, é inevitável nos perguntarmos que elementos de transformação de valores e hábitos vêm sendo evidenciados e se tornam relevantes ao ponto de, em algum momento, serem capazes de pressionar por mudanças na lei maior brasileira ou em sua interpretação e

aplicação. Este texto pretende elaborar uma reflexão dessa natureza a respeito do tratamento da privacidade pessoal, em particular no que concerne à proteção de dados pessoais.

No exame das transformações por que o entendimento social de privacidade vem passando, faz-se uso, neste texto, do Marco Civil da Internet, aprovado pelo Congresso Nacional e sancionado pela Presidente Dilma Rousseff na forma da Lei nº 12.965, de 23 de abril de 2014, como balizamento da discussão. O texto "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil", representando, segundo vários de seus defensores, uma norma de referência para a utilização da rede mundial a partir do nosso País, uma espécie de "constituição da internet".

Essa norma, muito aplaudida, está longe de ser consensual. Os conflitos que se caracterizaram desde o início da sua elaboração persistiram até sua aprovação e se prolongam no tempo. Representam, dentre outros, um confronto de interesses entre poderosos agentes econômicos envolvidos, de um lado, na oferta de conexão e acesso à rede e, de outro lado, no provimento de conteúdo aos seus usuários. As dificuldades para mediar esses conflitos de interesse dificultam a aprovação de leis congêneres em outros países. E tal aprovação foi viabilizada, no Brasil, por um ato de vontade da então Presidente da República, que se havia comprometido a promulgar essa lei até a data de realização do Net Mundial, evento realizado em São Paulo dedicado à governança da internet, e não admitiu a possibilidade de deixar de fazê-lo (OESP, 2014).

A lei, evidentemente, tem aspectos muito positivos, dada a qualidade das contribuições de um número expressivo de especialistas na sua elaboração e discussão. Porém, há disposições importantes em que persistem polêmicas por ora insuperáveis, sendo o tratamento da privacidade dos usuários da internet uma destas[1].

[1] Persistem controvérsias, também, em outros temas, como no tratamento da neutralidade de rede e na atribuição da responsabilidade de terceiros por conteúdo veiculado.

Esse caráter de incerteza quanto à doutrina jurídica aplicável à internet é bastante natural e não deve surpreender. A rede mundial consolidou-se e foi aberta ao público entre 1992 e 1994, após uma decisão do Congresso norte-americano. Trata-se, portanto, de um recurso que existe há apenas 25 anos. A internet passou, também, por diversas transformações e a forma atual de uso da rede, com preponderância do acesso móvel, teve início em 2001, com o lançamento dos primeiros Palm. Aplicações hoje dominantes tornaram-se relevantes na última década; o Facebook, provavelmente o serviço mais usado no momento, viu a luz em 2004. Tendências emergentes, como a computação em nuvem e a internet das coisas, poderão transformar o aspecto e o uso da rede mundial nos próximos anos, criando novos problemas de interpretação e aplicação da norma (LINS, 2013: 24, 33, 36-38).

O objetivo deste texto é discutir o problema do tratamento da privacidade em face da sua evolução social, alavancada pela presença dominante da internet. Adota-se um enfoque de economia política positiva, ou seja, de exame do comportamento dos agentes em face da norma e das motivações de ordem econômica capazes de induzir certas atitudes. Sua abordagem alinha-se à teoria positiva da regulação, remetendo ao trabalho seminal de Stigler (1971).

A aplicação da teoria econômica ao tratamento jurídico da internet vem dando lugar a uma linha de análise de grande interesse. A partir de textos exploratórios nos anos noventa, a exemplo de MacKey-Mason e Varian (1994), MacKey-Mason e Varian (1995), McKnight e Bailey (1997), surgiu uma vasta produção que se orienta segundo três ramos distintos: uma teoria normativa da regulação, que busca determinar as boas práticas no disciplinamento da oferta de serviços de acesso à rede e de tratamento de informações nesse contexto; um estudo dos efeitos sociais e macroeconômicos da internet e das perdas sociais decorrentes de falhas de mercado, em especial o chamado fosso digital; e um exame das práticas comerciais e de relacionamento na rede e sua evolução em decorrência de restrições regulatórias, com um enfoque de economia positiva.

Este trabalho procura contribuir com essa última linha de reflexão. Seu objetivo é examinar a evolução do comportamento dos agentes (usuários, provedores de conexão à internet e provedores de aplicações e conteúdo) quanto às práticas associadas à privacidade e a adequação à norma jurídica[2]. Este não é, então, um trabalho de exegese jurídica. Seu objetivo é sobretudo de discussão econômica, sendo eminentemente pragmático.

O texto é, portanto, especulativo: em lugar de voltar-se a uma apreciação das mudanças ocorridas na Constituição e na legislação infraconstitucional, tenta vislumbrar algumas pressões que virão a ser relevantes nos próximos anos. Esse caráter é inevitavelmente eivado de incerteza, na medida em que pequenos fatos escassamente percebidos na atualidade poderão ganhar uma relevância insuspeitada no futuro e temas que nos assombram poderão tornar-se inexpressivos. Trata-se, porém, de um esforço oportuno, pois traz ao debate aspectos de prazo mais dilatado que merecem consideração.

O trabalho está assim organizado: na próxima seção, discute-se o tratamento da privacidade no texto constitucional; na seção 2, a evolução de hábitos que poderão resultar em mudanças de caráter essencial no seu tratamento; na seção 3, as disposições gerais do Marco Civil a tal respeito; na seção 4, o problema da coleta encoberta de dados pessoais. A seguir, na seção 5, comentam-se os aspectos decorrentes do tratamento de grandes massas de dados. Apresentam-se, enfim, algumas conclusões.

1. Tratamento da privacidade na Carta

Privacidade é a garantia de assegurar a preservação da intimidade, da honra e da imagem do indivíduo, direitos da personalidade

[2] Observe-se que não será tratado o problema da coleta de dados obtidos fora dos limites da legalidade. Este texto não pretende alongar-se em aspectos penais da internet e, portanto, uma variedade de mecanismos de obtenção ilícita de dados deixará de ser analisada, tais como o rastreamento de dados no terminal do usuário mediante algum procedimento invasivo (vírus, cookies de rastreamento, cavalos-de-Tróia, applets, etc.), a obtenção de dados por monitoramento de linhas ou a solicitação fraudulenta de dados mediante mensagens enganosas.

reconhecidos na Constituição brasileira como fundamentais à integridade da pessoa[3]. O art. 5º da Carta, em seus incisos X a XII, estabelece:

> *"X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*
>
> *XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;*
>
> *XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;"*

A leitura desarmada desses comandos constitucionais esconde grande complexidade interpretativa e de aplicação. No grau mais próximo da individualidade em sentido estrito é reconhecido o direito da pessoa a preservar sua integridade física e moral, suas crenças, sua imagem e seus elementos distintivos de identidade. Já em um contexto de intimidade mais amplo, a garantia de privacidade protege elementos adicionais da vida particular, incluindo-se dentre estes os hábitos, as práticas, os encontros episódicos, os registros audiovisuais da vida pessoal ou familiar e as expressões verbais e escritas de ideias e convicções, quando conduzidas e expressadas entre familiares, amigos e associados. E, em âmbito ainda mais alargado, a privacidade alcança as relações do indivíduo com a coletividade e com os serviços públicos, nos aspectos que possam vir a atingir a integridade individual, tais como registros públicos ou particulares de rendimentos, propriedade,

[3] Tal construção jurídica não é fortuita ou desprovida de um contexto maior. O reconhecimento dos direitos da personalidade advém de um debate ético e político de grande alcance, cuja explanação escapa aos objetivos deste texto, e se expressa em diversos textos e acordos, a exemplo da Declaração Universal dos Direitos Humanos da ONU, que estabelece, em seu art. 12: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

situação financeira, práticas religiosas, situação profissional, de saúde ou de relacionamentos com terceiros[4].

Na sociedade contemporânea, um elemento central do debate da privacidade envolve a coleta e a divulgação de informações a respeito da pessoa, ou seja, de dados pessoais. A delimitação do que seja dado pessoal varia de acordo com jurisdições e com o alcance das normas legais, sendo um debate complexo, mas uma possível definição é a do art. 2º da Convenção de Estrasburgo de 1981[5], que define dado de caráter pessoal em sentido amplo, como "qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação ('titular dos dados')". Dados de caráter pessoal, segundo o art. 5º da Convenção, devem ser obtidos e tratados de forma leal e lícita, registrados com fim determinado e conservados por período que não exceda à finalidade do seu registro.

Feitas essas considerações de caráter geral para contextualizar o problema, este texto não pretende aprofundar ou esgotar um debate sobre a natureza e o tratamento jurídico de dados pessoais. O leitor interessado em aprofundar essa discussão tem a seu dispor ampla literatura. Sugere-se, como um primeiro passo, recorrer a um dos muitos textos disponíveis de juristas de renome, tais como Gomes (1983: 126-143), Ferraz Júnior (1993) ou, no aspecto mais específico do direito aplicado à internet, o interessante trabalho de Paesani (2014). Basta aqui constatar que a privacidade é usualmente considerada em vários níveis ou camadas que se sobrepõem, alcançando um conjunto crescente de atividades em que o indivíduo se engaja.

[4] Há várias interpretações e variantes dessa teoria das esferas, divulgada sobretudo a partir de Hubmann (1957: 524). Trata-se de construção de certo interesse para comparar a gravidade de diferentes formas de ofensa à intimidade, subsidiando o debate do tema e a formalização legal da proteção aplicável. É uma abordagem que traz vantagens analíticas quando comparada ao enfoque linear que nasce da concepção de Warren e Brandeis (1890) da privacidade como o direito de ser deixado a sós.

[5] A Convenção foi assinada no contexto de uma série de tratados do Conselho da Europa (CE, 1981).

2. A privacidade hoje

Em 2012, *selfies* de uma conhecida atriz brasileira nua foram divulgadas na internet, provavelmente após uma invasão de seu *smartphone*. O episódio rendeu um alentado debate sobre a exposição de pessoas na internet e resultou na aprovação da Lei nº 12.737, de 30 de novembro de 2012, que acresceu ao Código Penal a tipificação da conduta de invasão de dispositivo informático. A lei passou a ser conhecida como Lei Carolina Dieckmann.

Não se trata de um episódio isolado. Registros de *nudes* ou de imagens com conotação sexual vazadas na internet são frequentes e atingem principalmente mulheres, expondo-as a constrangimentos. De atrizes e *socialites* notórias a adolescentes desconhecidas, contam-se aos milhares as vítimas de ofensa com o uso da internet, configurando um problema ético relevante e orientando o debate sobre privacidade nos dias atuais. O discurso do confronto entre privacidade e internet tem sido focado na proteção da individualidade das pessoas e da sua vida particular, em oposição ao caráter invasivo da rede e à disseminação fora de controle das informações pessoais.

Por outro lado, a exposição compulsiva da vida privada tornou-se uma característica da vida digital. O modo de operação das redes sociais mais populares induz os usuários a compartilhar experiências e sentimentos pessoais em mensagens e imagens que, não raro, são repercutidas, admiradas e copiadas por milhares de seguidores. Vivemos um momento em que notoriedade se tornou um valor social relevante.

A privacidade na internet perpassa todas essas dimensões na medida em que muitas das atividades antes realizadas inteiramente no “mundo físico” passaram a ter um mapeamento no “mundo virtual”. Essa extensão, projeção ou transferência decorre de alguns processos que se consolidaram na medida em que a rede mundial se expandiu e tornou-se um ambiente que envolve os usuários e intermedeia suas relações com as demais pessoas e com as instituições, mediante aplicativos, ambientes de relacionamento e repositórios de informações.

Os fundamentos da privacidade na internet não escapam aos princípios gerais estatuídos na norma constitucional. Alcançam a intimidade, a vida privada, a honra e a imagem das pessoas, seu domicílio e suas comunicações. No entanto, trazem novos elementos ao debate por três razões associadas ao tratamento e ao uso de dados pessoais.

Em primeiro lugar, há procedimentos de individualização que prescindem do conhecimento da identidade da pessoa. Pode-se, por exemplo, acompanhar o terminal de acesso à rede que este utiliza, seja um *smartphone*, um *tablet* ou um computador. Na medida em que o acesso tende a ser contínuo, as ações e procedimentos executados pelo aparelho acabam por refletir a movimentação e as decisões do usuário e incorporar-se à sua identidade. Não é preciso saber que o celular pertence “a fulano”. Pode-se construir o perfil do “proprietário do terminal” a partir das informações que este posta nas redes sociais, das compras que faz pelos aplicativos de mercado de trocas, das consultas que marca em hospitais ou clínicas por mensagens eletrônicas, dos trajetos que percorre e são rastreáveis por seu GPS.

Em segundo lugar, é possível obter informações a respeito do usuário sem que este saiba disso e consinta com o procedimento, ou, mesmo que supostamente saiba, aceite e consinta, sem que esteja de fato consciente do alcance dessa autorização. A inserção de *cookies*, pequenos arquivos que registram procedimentos do usuário, é um exemplo desse tipo de mecanismo. A utilização do arquivo pode ser autorizada ou negada, mas usualmente o usuário desconhece em detalhes o tipo de informação coletada, o uso feito desta e a periodicidade de atualização do dado e do seu acesso por terceiros.

Em terceiro lugar, enfim, dados coletados e armazenados podem permanecer disponíveis por tempo indeterminado, podem ser reprocessados ou cruzados para criar novos dados, podem ser remanejados, cedidos ou comercializados. Seu ciclo de vida é diferente do ciclo de vida da pessoa a que se referem. Episódios da vida pregressa, de relações anteriores, da infância e da juventude, podem voltar a circular na rede, prejudicando alguém

que eventualmente tenha mudado de atividade, de ambiente, de hábitos ou de opinião.

A constatação desses novos elementos tem gerado efeitos no avanço da doutrina, no debate legislativo e nas decisões judiciais. Não se pretende aqui fazer uma resenha dessas contribuições, inevitavelmente longa e complexa. Deseja-se agregar a esse debate um aspecto bastante discutido, que poderá ter implicações importantes para a interpretação da norma constitucional e da legislação infraconstitucional: o significado econômico da privacidade e da transformação pela qual está passando.

3. O caráter econômico dos dados pessoais e a abordagem do Marco Civil da Internet

Além do caráter social e de dignidade pessoal, a privacidade tem motivações e implicações econômicas importantes. Do ponto de vista econômico, importa delimitar em que medida a privacidade representa um ativo para o indivíduo.

Trata-se, por um lado, de uma garantia que assegura sua condição de acesso ao mercado, ou seja, que protege sua imagem pública tornando-o um parceiro palatável para transações comerciais e sociais, caracterizando o que Ferraz Júnior (1993: 440) denomina interesse. Por outro lado, é um mecanismo que garante ao titular o controle sobre suas informações pessoais, dando-lhe o benefício, *a priori*, de dispor sobre seu uso. Nesse sentido, a privacidade é condição para assegurar a propriedade sobre dados pessoais enquanto bem precificável, do qual o titular possa dispor e que possa comercializar com vantagens.

O preço desses dados é estabelecido por relações de mercado. Há duas situações distintas a considerar. Uma é a da pessoa notória, cujo dado pessoal tem um valor estabelecido pela demanda específica de informações disseminâveis e vendáveis acerca dessa pessoa. Trata-se de informação cujo valor inerente é suficientemente alto para que esta possa ser transacionada[6].

[6] Um exemplo trivial é o de celebridades que cobram cachê por entrevistas, prática bastante usual, por exemplo, na imprensa britânica.

Outro é da pessoa mediana, cuja relevância individual se equipara à dos demais membros da coletividade. Nesse caso, sua informação individualizada tem escasso valor comercial, pois este nascerá da agregação de dados em massa, que poderá apontar tendências, preferências ou comportamentos coletivos. Usualmente, nesses casos, a "compra" do dado resulta da sua troca por serviços ou acessos.

O Marco Civil da Internet trata especificamente dos direitos assegurados mediante a privacidade em quatro grupos de artigos. Os arts. 7º e 8º delimitam as garantias dos usuários em termos de direitos da personalidade e tratamento de dados pessoais. Os arts. 10 e 11 definem critérios de guarda e proteção de dados pessoais. Os arts. 13 a 17 tratam da coleta e guarda de registros de conexão e de acesso a aplicações. O art. 12, enfim, da aplicação de penalidades por descumprimento das disposições da lei.

O exame do art. 7º nos ajuda a contextualizar a delimitação conceitual de intimidade e privacidade no âmbito da internet:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> .....
>
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
>
> .....”

Tais disposições trazem bastante clareza ao tratamento dado a informações pessoais disponibilizadas pelo usuário, ou seja, ao fornecimento declarado de informações pessoais, ou coletadas no âmbito da prestação do serviço.

Quando a informação é requerida ao usuário – por exemplo, para seu cadastramento em uma aplicação – ou coletada para registro do seu acesso à rede ou a um serviço ou aplicação, as disposições do art. 7º se aplicam integralmente. O usuário deve ser avisado dos termos de uso, dos critérios de coleta, armazenamento, utilização e disseminação dos dados pessoais e deve ser garantida sua exclusão definitiva quando cessar a relação entre as partes.

Um aspecto importante é o de que o consentimento expresso sobre uso de dados pessoais sobrepõe-se a outras disposições da lei (inciso VII). Daí a importância da leitura dos termos de uso de uma aplicação, procedimento que a maior parte dos usuários deixa de fazer com atenção.

No entanto, há dificuldades de entendimento e de enquadramento de outras situações, que serão descritas a seguir. Dado que grande parte das aplicações relevantes destina-se à troca de informações entre

seus usuários ou a divulgação ampla de opiniões e registros – o que se denomina popularmente rede social –, é importante estabelecer, nesse extenso rol de informações disseminadas pelo usuário, o que se caracteriza como dado pessoal para os fins da lei e que informações são abraçadas sob a proteção da privacidade. Estes são temas controversos[7].

Na jurisprudência norte-americana, por exemplo, é recorrente a tese de que a referência a uma pessoa no contexto de uma publicação ou divulgação não comercial estará rompendo sua privacidade somente se divulgar "fatos privados". Segundo Paton-Simpson (1998: 319), essa teoria baseia-se em duas premissas: fatos reconhecidos como "públicos" devem ser excluídos da proteção da privacidade e a divulgação pode ser desagregada em fatos singulares que serão, um a um, reconhecidos como públicos ou privados. A autora questiona essas assertivas, apontando que, por um lado, é questionável a classificação de um fato como público pelo mero fato de ter sido previamente registrado ou divulgado, porque o titular pode desejar, ainda assim, restringir ou questionar sua divulgação ulterior, de modo a limitar danos à sua personalidade decorrentes da repetição do fato em maior escala[8] (1998: 321-322). E, por outro lado, que a desagregação ou atomização da informação divulgada pode comprometer a compreensão acerca do alcance do dano potencial que acarreta, pois a identificação de condições de contorno da apuração ou de inferências ou correlações sugeridas ficará prejudicada. O todo, em suma, pode ser maior do que as partes (1998: 331-333).

[7] Castro (2002: 42) aponta que não se deve limitar o escopo da análise a informações pessoais diretamente consideradas, mas estendê-lo a "todo tipo de informações que indiretamente possam ser associadas a uma pessoa, por exemplo, um número de telefone, uma placa de automóvel, um endereço de e-mail". O autor aponta ainda que dados de caráter pessoal incluem também informações, ainda que anônimas, que permitam, mediante cruzamentos ou associações, delimitar a identificação do titular.

[8] A autora cita vários exemplos e decisões para fundamentar o argumento e questionar a distinção entre público e privado. Um exemplo trivial é o de uma mulher vítima de violência: a divulgação de sua identidade em um jornal local torna seu nome "público", mas a ulterior disseminação dessa informação em outros veículos pode ser-lhe crescentemente danosa. Há também graus do que seja público: um registro em cartório é público, porém é menos divulgado e menos acessível do que uma reportagem de jornal ou um *tweet*. O argumento é o de que uma informação, ainda que pública, pode guardar elementos de vínculo à personalidade e sua crescente divulgação pode ferir a privacidade da pessoa.

Uma alternativa é a de enumerar exaustivamente na lei o rol de informações que podem ser consideradas como dados pessoais. Tal abordagem, porém, não considera que a proteção à privacidade não alcança apenas os dados pessoais arrolados em lei, mas qualquer dado que afete as esferas íntima ou privada do titular. Ademais, uma delimitação demasiadamente ampla do que seja dado pessoal, a depender do alcance considerado, poderá impor um ônus a qualquer comentário ou divulgação jornalística, prejudicando o interesse público[9]. Além disso, há que se considerar que certas informações serão pessoais, na prática, somente quando colhidas ou usadas em certo contexto e associadas inequivocamente ao titular, de modo que um tratamento uniforme da sua proteção em qualquer circunstância terá o efeito de onerar desnecessariamente atividades prosaicas com exigências descabidas.

Outra alternativa é a de confrontar princípios gerais, como o interesse público ou o benefício econômico e social da divulgação, com a garantia de privacidade. Nesse contexto, a aplicação da privacidade é delimitada como aquela condição em que outras pessoas deixam de ter acesso a alguma informação acerca do titular ou deixam de viver alguma experiência com o titular ou a ele correlata. Trata-se também de alternativa controversa, pois requer o cotejamento dos ganhos que o titular aufere, graças à preservação da vida privada e da intimidade, com as perdas dos demais, decorrentes da restrição imposta, procedimento viável no lento ritmo da decisão judicial, mas inaplicável às rápidas disseminações virais da internet.

4. A coleta encoberta de dados pessoais pelo provedor de conexão

Dados acerca do usuário podem ser coletados ou criados sem seu conhecimento ou consentimento, o que se denomina de coleta encoberta. E, em vários casos, isto é efetuado dentro dos limites da legalidade e, eventualmente, propicia benefícios ao próprio usuário e ao mercado. Sua

[9] Um exemplo prosaico é o da obtenção de licença do fotografado para uso da imagem. Isto faz sentido para a disseminação de uma imagem publicitária que faz uso do trabalho de um modelo, mas é um exercício fútil se aplicado a uma fotorreportagem, visto que não há, por exemplo, como obter autorizações de todas as pessoas identificáveis em uma multidão que comparece a um ato público.

vedação ou regulamentação, portanto, deve ser cuidadosamente cotejada com uma eventual perda social correspondente.

O caso trivial é o de dados que o próprio Marco Civil obriga a armazenar, sem prévia autorização do usuário. No acesso à rede, a lei impõe a coleta de um conjunto de indicadores da transação:

> "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> ....."

Trata-se de um ônus para o provedor de conexão, pois implica na coleta e preservação de dados sem valor comercial, ao ser restringido o seu uso (vide art. 7º, inciso VII) e imposta sua manutenção sob sigilo.

A lei veda, além disso, que o provedor de conexão à internet mantenha um *log* das transações do usuário com provedores de aplicação:

> "Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet."

Do ponto de vista econômico, portanto, o provedor de conexão fica limitado na coleta e acumulação de informações que tenham valor comercial, precisamente as que refletem as preferências reveladas pelo usuário, ficando frustrada a possibilidade de agregá-las.

Há, ainda assim, outras oportunidades de captura e coleta encoberta de dados do usuário. Há duas conjunturas em que o problema se torna mais complexo. Uma é a da informação desvinculada da pessoa e armazenada cumulativamente em caráter anônimo, sem possibilidade de reconstrução do vínculo. A outra é a da informação em fluxo, que é criada, usada de imediato e em seguida descartada.

O primeiro é o caso de dados "anonimizados", que são depurados da identidade do titular, sendo agregados no momento de sua ocorrência. O argumento que fundamentaria a legalidade dessa coleta é o de que, uma vez detectada, por exemplo, a transação de um usuário com uma

aplicação, essas informações seriam tratadas como anônimas, ou seja, a identidade do usuário seria extirpada. Mais ainda, sendo impossível a identificação deste, é irrelevante a obtenção de licença para a coleta do dado, vez que uma eventual invasão da privacidade seria improvável. A coleta encoberta seria, portanto, viável.

Nesse aspecto, um dos espaços comerciais mais interessantes é a coleta de dados relacionados ao terminal de acesso à internet, em especial se este for um *smartphone* que acompanha o usuário em caráter contínuo e permanente.

O argumento para admitir essa coleta baseia-se em três premissas. A primeira é a de que é possível tratar o terminal como a entidade destinatária das ofertas decorrentes da coleta, sem entrar no mérito da identidade do titular. Este é apenas um “alguém” cujos trajetos e cujas decisões de uso da rede são conhecidas, mas sobre cuja real identidade não se faz qualquer conjectura. A segunda premissa é a de que é possível tratar e combinar essas informações como se fossem anônimas, ou seja, efetivamente desagregadas da identidade do titular. A terceira, de que ao menos parte dessas informações seria decorrente da detecção de parâmetros do próprio aparelho terminal, tais como posição geográfica, tempo de uso, volume de tráfego com a rede, não caracterizando dados de acesso a aplicações.

Há duas dificuldades no tratamento desses argumentos. A primeira é a de que a coleta, sendo encoberta, não garante que o usuário seja preservado. Os direitos do usuário estariam nas mãos de alguém que sequer se qualifica a uma relação contratual bilateral explícita. O provedor pode, simplesmente, desrespeitar o anonimato e o usuário não teria elementos para constatar o fato. A segunda, a de que uma combinação de informações poderia levar à identificação do usuário, ou pelo menos ao seu enquadramento em um perfil, apesar dos esforços do provedor. Estaria sendo, nesse caso, prejudicada sua privacidade. O pareamento entre o usuário e o terminal pode resultar na identificação do primeiro e em eventual quebra de privacidade. Há também a necessidade de deixar esclarecida a natureza dos dados de terminal, dirimindo

dúvidas quanto ao seu enquadramento ou não como parte do registro de conexão[10].

O segundo caso, da criação de dados a partir de informações em fluxo, é outra modalidade de coleta de dados pessoais que pode não ser alcançada pelas disposições do Marco Civil da Internet. Refere-se ao processamento de informações ou à construção de informações a partir de ações do usuário, no momento em que estas ocorrem[11].

Se essa informação criada for armazenada junto com uma identificação do usuário, recairemos no debate anterior: trata-se de algo que o titular não imaginou existir ou ser coletável, estando fora do seu domínio de controle, mas de fato existe e se refere à sua pessoa. Portanto, o debate sobre a privacidade se restabelece. No entanto, informações em fluxo em geral são descartadas após a criação, para se evitar custos crescentes de armazenamento, ficando preservados apenas os indicadores produzidos e agregados. Portanto, não há guarda, nos termos vedados pela lei.

Do ponto de vista econômico, há implicações quanto às oportunidades de prestação de serviços ao usuário a partir dessas informações, seja mediante aplicações (nesse caso remetemos ao debate dos dados de aplicações, que serão tratados na seção 5 deste texto), seja pelo provedor de conexão. No caso do registro de conexão, porém, o Marco Civil da Internet impõe um mau negócio para todos. Embora o problema do provedor de conexão seja o de incorrer no custo de coleta e armazenamento dos dados desagregados

[10] Esses questionamentos referem-se ao uso de sinalização trocada entre o terminal e a infraestrutura de rede, sendo inteiramente diferentes do problema do recolhimento do aparelho e da captura do seu conteúdo, ações cuja legalidade pode ser discutida com base na teoria sugerida, por exemplo, por Freire e Sales (2015: 571-572), que equipara o terminal de acesso à rede com o domicílio do usuário, por acolher seus dados pessoais e revelar seus hábitos, práticas e preferências.

[11] Suponha, por exemplo, que um sistema de dispensa de numerário (caixa eletrônico) identifique, nas imagens dos usuários que acessam seu sistema, elementos que permitam o reconhecimento de padrões de satisfação, preocupação e assim por diante. Esses registros podem ser armazenados para várias aplicações. Trata-se de um caso de coleta de uma informação pessoal de fluxo, ou seja, no momento em que a transação está ocorrendo. A informação em si – a feição do usuário – é irrelevante, mas a informação criada – a sensação presumida – pode ter valor comercial significativo. Este, como outros exemplos citados, é inteiramente fictício, sugerindo mais uma possibilidade de ocorrer do que propriamente uma prática já existente.

acerca da conexão, sem obter receitas dos mesmos, o problema do usuário final é o de ter essas informações armazenadas por terceiros para fins de eventual investigação sem que isto resulte em qualquer utilidade ou benefício para si. De fato, ele já paga pelo acesso ou, quando o obtém gratuitamente, é parte da audiência potencial de propaganda, comercializável pelo provedor. A coleta dos dados de conexão não é contrapartida comercial do serviço.

5. Privacidade, "big data" e dados colhidos por aplicações

O Marco Civil da Internet assegura aos provedores de aplicações a coleta e uso de dados do usuário, nos termos previstos em seus arts. 15 e seguintes:

> "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> .....
>
> Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
>
> I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou
>
> II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular."

De modo geral, as regras consagradas no Marco Civil para provedores de aplicações assemelham-se às impostas aos provedores de conexão, com duas diferenças importantes. Em primeiro lugar, é admitida a guarda de registros de acesso a outras aplicações, desde que previamente consentida pelo usuário (art. 16, inciso I). Em segundo lugar, há, na prática, a coleta e armazenamento de informações oferecidas pelo próprio usuário. Se, no primeiro caso, a aplicação das garantias enumeradas no art. 7º não guarda novas dúvidas em relação à discussão da seção 5, no segundo caso há outras considerações a examinar.

Um grande número de usuários da rede tem como prática a postagem de informações e opiniões as mais variadas em redes de relacionamento público. Embora, em alguns casos, quem posta essas mensagens se acautele quanto ao público que as recebe, sua audiência tende a ser mais ampla do que o esperado por dois motivos: a reprodução dessas mensagens por terceiros – a exemplo do comando *retweet* no aplicativo Twitter – e os mecanismos de rastreamento operados por terceiros.

Informações desse tipo tendem a ser muito diversificadas, envolvendo desde fotografias das férias até opiniões sobre fatos políticos, alcançando aspectos os mais variados da vida das pessoas. Um exame minucioso de um perfil em rede social e das mensagens postadas pode revelar detalhes extremamente íntimos de uma pessoa: endereço, parentes, filhos, relacionamentos, contas de banco, poder aquisitivo, preferências de consumo, temperamento, estado de saúde, escolhas religiosas e por aí vai. A maior parte dos usuários da internet levaria um susto se fosse confrontada ao grau de indiscrição a que se sujeitam em decorrência das informações que eles próprios divulgam.

Mecanismos de rastreamento são utilizados para monitorar usuários ou para estabelecer indicadores a partir da análise de perfis. Esse tipo de rastreamento é realizado rotineiramente pelo próprio provedor da aplicação, inclusive para melhor atender ao usuário. Por exemplo, em lojas virtuais, o rastreamento de buscas e de compras anteriores permite que melhores sugestões sejam oferecidas ao interessado durante suas pesquisas. Programas de terceira parte também podem realizar essa navegação de dados publicados, usualmente para consolidar indicadores ou mapear informações agregadas de uso da internet.

A dificuldade para enquadrar esse uso das informações no contexto dos dados pessoais protegidos resulta do fato de estas terem sido postadas pelo próprio usuário. A depender das cláusulas do contrato de adesão ao serviço – que a maior parte dos usuários furta-se a ler –, tais informações tornam-se, a rigor, públicas. Na política de dados do Facebook, por exemplo, é

esclarecido que essas informações são compartilhadas com as pessoas com quem o usuário compartilha e se comunica, com pessoas que visualizam conteúdos que outras pessoas compartilham sobre o usuário, com aplicativos, sites e integrações de terceiros que usam ou são integrados aos serviços do Facebook, com as empresas e parceiros do Facebook e com serviços de publicidade, medição e análise, neste último caso na forma de informações pessoais não identificáveis (FACEBOOK, 2016). A plataforma oferece ao usuário recursos variados para limitar a disseminação de suas informações, transferindo-lhe assim a responsabilidade sobre esse controle, mas isto não elimina o fato de que uma autorização contratual ampla esteja dada.

O grande desafio proposto por essa modalidade de armazenamento de dados refere-se, porém, ao que vem sendo chamado de “big data”. Trata-se da coleta ou da construção de dados a partir de informações disponíveis no ambiente da rede internet, de bancos de dados ou de ações de usuários, usualmente em tempo real. Na maior parte das situações em que essa abordagem é usada, não se pretende consolidar um banco de dados estável para subsidiar a tomada de decisões baseada em fatos. Ao contrário, o que se espera é tratar de modo dinâmico e temporário essas informações para colher sugestões de alternativas a explorar.

A expansão dos recursos computacionais e o desenvolvimento de soluções para tratamento de grandes volumes de informações, em especial após o 11 de setembro, viabilizaram o rastreamento e a mineração de dados em grande escala. A extensão dessas práticas é de tal ordem que o indivíduo não tem a menor possibilidade de identificar e controlar a proteção de seus dados pessoais. Eles simplesmente se espalham pela rede, em sucessivos episódios de manipulação (MUNDIE, 2014: 29-30). A capacidade de intersecção entre essas informações é tão sofisticada que, não raro, programas de análise de dados colhem evidências sobre as pessoas que elas mesmas não seriam capazes de imaginar ou perceber. Sabem mais sobre nós do que nós mesmos.

O usuário, em suma, teria mais vantagens se lhe fosse dada a garantia de que todos os seus dados estivessem armazenados em um local bem determinado e que os usos autorizados para esses dados fossem bem delimitados. Seus dados seriam colhidos por *wrappers*, programas que os usariam e reordenariam para finalidades bem estabelecidas. Por ora, um esquema como este é ainda inviável, seja por questões econômicas (o depositário desse dado teria benefícios e encargos diferenciados e operaria em um mercado de comercialização de dados de formato ainda inexistente), seja por questões de caráter legal (seria necessário um acordo global de tratamento de dados segundo esse formato e punições para quem se desviasse desse formato de coleta e uso de dados pessoais). Desnecessário apontar que esquemas desse tipo demandariam uma terceirização do armazenamento de dados pessoais, não admitida no Marco Civil, em vista da combinação do art. 7º, VII, com os arts. 13 e 15.

Destaque-se que os provedores de aplicações, contrariamente aos provedores de conexão, dispõem de um mercado de comércio de dados, unicamente em decorrência da natureza do serviço prestado ao usuário. De fato, o provedor de aplicações administra um extenso conjunto de dados abertos postados pelo usuário, cuja exploração ulterior é garantida por uma autorização ampla, sendo esta a moeda de troca para beneficiar-se do serviço. O Marco Civil reconhece a prevalência dessa autorização sobre outras proteções previstas, possibilitando assim a criação de perfis muito elaborados acerca de usuários e terminais de acesso e sua oferta a terceiros[12].

Em termos de custos, deve ser enfatizado que os provedores de conexão e de aplicações devem assegurar proteção razoável aos dados armazenados, prevenindo-se contra sua obtenção ilícita. Isto envolve custos de segurança relacionados com a prevenção contra acessos indevidos aos seus repositórios e decodificação do conteúdo acessado. Envolve também

[12] Um exemplo é o da plataforma Google. Ao associar as buscas e acessos ao catálogo com dados dos usuários, o Google pode cobrar por serviços de preferência na oferta de opções (os "sites patrocinados"), pela distribuição de publicidade a sites conforme o número de acessos ("google ads") e assim por diante, estruturando uma família de aplicações destinadas ao usuário final, a outros provedores e a anunciantes em geral.

redundância de dados para evitar perdas em caso de incidentes. Impõe, em suma, investimentos em capacidade computacional, monitoramento de suas comunicações e software de proteção, que são crescentes em relação ao aumento de capacidade da rede, do tráfego de dados e do número de usuários atendidos.

Nesse aspecto, vale ressaltar que o provedor de aplicação dispõe da alternativa de decidir, a partir da eficiência econômica, se é vantajoso ou não expandir a coleta de informações de usuários. Provedores individuais ou não comerciais, em particular, são isentos dessa obrigação, excetuados os casos de determinação judicial. E os prazos de guarda são menores do que os impostos aos provedores de conexão à internet. Estes últimos, de sua parte, estão presos por uma camisa de força regulatória, conforme anteriormente apontado.

CONCLUSÕES

Embora este texto tenha se estendido a respeito das disposições da Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, o objetivo desse esforço foi o de contextualizar considerações quanto aos efeitos desse normativo sobre os interesses econômicos dos titulares de dados pessoais, dos provedores de conexão à internet e dos provedores de aplicações na rede.

Buscou-se apontar vantagens e restrições estabelecidas pelo Marco Civil e alternativas de ação disponíveis a esses agentes, para contornar as determinações da lei.

Em linhas gerais, de um ponto de vista de economia política, os seguintes pontos podem ser reforçados: a coleta compulsória de dados pessoais de acesso, sem benefícios correlatos, reduz a percepção de bem-estar do usuário; a assimetria de tratamento entre provedores de conexão e provedores de aplicações estende-se tanto ao alcance dos dados que podem ser coletados quanto à liberalidade em usá-los, haja vista a disseminação de informações pelo

próprio usuário e as políticas de uso a que este adere; a pressão por investimentos crescentes em capacidade de tráfego recai sobre os provedores de conexão, levando-os a reexaminar procedimentos de cobrança e de captura de ganhos; a responsabilidade pela preservação dos dados é dos próprios provedores, dificultando a implantação de esquemas de tratamento compatíveis com a realidade do tráfego de informações na rede e de práticas de *data mining*, a cada dia mais utilizadas.

Para o indivíduo, vem surgindo uma nova realidade em que os pressupostos de privacidade e de proteção da pessoa vêm sendo corroídos por uma crescente exposição pública de informações a seu respeito. Com o agravante de que tal exposição decorre do uso de dados que o próprio titular concordou em compartilhar, ainda que sem uma percepção do alcance dessa licença, ou de dados construídos a seu respeito. Os desafios ao tratamento da privacidade pessoal, em suma, tenderão a assumir novo colorido nos próximos anos, exigindo reinterpretações da norma constitucional. Estamos no limiar de um mundo novo, um mundo da vida absolutamente pública.

REFERÊNCIAS BIBLIOGRÁFICAS

BOYD, danah m. e Nicole B. ELLISON (2008). “Social network sites: definition, history, and scholarship”. *Journal of Computer-Mediated Communication*, 13: 210–230.

BRASIL (1988). **Constituição da República Federativa do Brasil**.

BRASIL (2014). **Lei nº 12.965, de 23 de abril de 2014**. “Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil”.

CASTRO, Luiz F. (2002). “Proteção de dados pessoais – internacional e brasileiro”. *Revista CEJ*, 6 (19): 40-45.

Conselho da Europa – CE (1981). **Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal**. CETS nº108. Disponível em: http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108. Acessado em 21/4/2016.

Facebook (2016). **Política de Dados**. Disponível em: https://www.facebook.com/about/privacy. Acessado em 29/3/2016.

FERRAZ Jr., Tércio S. (1993). “Sigilo de dados: os direitos à privacidade e os limites à função fiscalizadora do Estado”. *Revista da Faculdade de Direito da Universidade de São Paulo*, 88: 439-459.

FREIRE, Geovana M. e Tainah S. SALES (2015). “Os direitos à identidade digital e ao acesso à internet como instrumentos de concretização dos objetivos de desenvolvimento do milênio e da democracia”. *Revista Justiça do Direito*, 29 (3): 563-586.

GOMES, Orlando (1983). **Introdução ao Direito Civil**. 7ª ed. Rio: Forense.

HUBMANN, Heinrich (1957). “Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion”. *Juristen Zeitung*, 12 (17): 521-528.

LINS, Bernardo E. (2013). “A evolução da internet: uma perspectiva histórica”. *Cadernos Aslegis*, 17 (48): 11-45.

MACKIE-MASON, Jeffrey K. e Hal VARIAN (1995). "Pricing Congestible Resources". *IEEE Journal of Selected Areas in Communications*, 13 (7): 1141-1149.

MACKIE-MASON, Jeffrey K. e Hal VARIAN (1994). "Pricing the Internet". Em: KAHIN, Brian e James KELLER (orgs.). **Public Access to the Internet**. Cambridge, MA: MIT Press, p. 269-314.

MCKNIGHT, Lee W. e Joseph P. BAILEY (1997). “An introduction to Internet economics”. Em: MCKNIGHT, Lee W. e Joseph P. BAILEY (orgs.). **Internet Economics**. Cambridge, MA: MIT Press, p. 3-24.

MUNDIE, Craig (2014). “Privacy pragmatism: focus on data use, not data collection”. *Foreign Affairs*, 93 (2): 28-38.

O Estado de São Paulo (2014). “Senado aprova Marco Civil da Internet: projeto foi aprovado por unanimidade e agora segue para sanção da presidente Dilma Rousseff”. Disponível em: http://blogs.estadao.com.br/link/senado-aprova-marco-civil-da-internet/. Acessado em 10/5/2015.

PAESANI, Liliana M. (2014). **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil**. 7ª ed. São Paulo: Atlas.

PATON-SIMPSON, Elizabeth (1998). “Private circles and public squares: invasion of privacy by the publication of ‘private facts’”. *The Modern Law Review*, 61 (3): 318-340.

SCHWAB, Klaus (2016). **The Fourth Industrial Revolution**. Genebra: World Economic Forum.

STIGLER, George J. (1971). “The theory of economic regulation”. *Bell Journal of Economics and Management Science*, 2 (1): 3-21.

TIGRE, Paulo B. (2014). “De Babbage a Zuckerberg: uma breve história das tecnologias da informação e seus impactos na indústria”. In:cgi.br. Pesquisa sobre o uso das tecnologias da informação e comunicação no Brasil: TIC domicílios e empresas 2013. São Paulo: Comitê Gestor da Internet no Brasil, pp. 129-135.

WARREN, Samuel D. e Louis D. BRANDEIS (1890). “The Right to Privacy”. *Harvard Law Review*, 4 (5): 193-220.

2018-775