

DIREITO À PRIVACIDADE E A REGULAÇÃO DA COMUNICAÇÃO DIGITAL NO BRASIL, EUA E UNIÃO EUROPEIA

RIGHT TO PRIVACY AND THE REGULATORY FRAMEWORK FOR DIGITAL COMMUNICATION IN BRAZIL, THE UNITED STATES AND THE EUROPEAN UNION

Sivaldo Pereira da Silva*

RESUMO:

Este artigo analisa o atual cenário regulatório da comunicação digital e suas repercussões na concepção do direito à privacidade. O objetivo é desenvolver um quadro analítico-comparativo sobre o tema no âmbito das políticas de comunicação. Primeiramente, discute-se a configuração conceitual da privacidade enquanto direito e seus subsequentes horizontes frente ao fenômeno das tecnologias digitais. Em seguida, observa-se o corrente quadro regulatório em três âmbitos geopolíticos: Brasil, EUA e União Europeia. Além da revisão de literatura em teoria social, o estudo foi baseado na consulta de leis, decretos, normas infralegais, relatórios governamentais, jurisprudência e outras normatizações. Os resultados demonstram que a ideia tradicional de privacidade tem sofrido abalos conceituais diante das inovações trazidas pela comunicação digital. No atual cenário, não há uma padronização nos modelos de regulação vigentes: ocorre um quadro regulatório fragilizado e pouco desenvolvido nos EUA, mais consolidado na Europa e em implementação no Brasil.

PALAVRAS-CHAVE: Regulação da Internet. Privacidade. Comunicação digital e direitos humanos.

ABSTRACT:

This article analyzes the current regulatory scenario of digital communication and its impacts on the right to privacy understanding. The goal is to develop an analytical-comparative table on the topic in the context of communication policies. First, we discuss the conceptual construction of privacy as a right and its derived horizons related to digital technologies. Second, we analyze the current regulatory framework considering three geopolitical areas: Brazil, the USA and the European Union. In addition to the

* Professor do Curso de Jornalismo da Universidade Federal de Alagoas (UFAL) e do Programa de Pós-Graduação em Comunicação da Universidade de Brasília (UnB). ALAGOAS, Brasil. sivaldop@decos.ufal.br

literature review on social theory, the study is based on consultation laws, decrees, regulatory provisions, government reports, case law and other norms. The results show that the traditional idea of privacy has been modified by digital communication innovations. In the case of geopolitical scenarios, there is no standardization in the existing regulation models: There is a fragile and underdeveloped regulatory framework in the US, there is a consolidated regulatory framework in Europe and there is an initial implementation in Brazil.

KEYWORDS: Internet regulation. Privacy. Digital Communications and Human Rights

INTRODUÇÃO

O desenvolvimento da comunicação digital nas últimas décadas e o crescimento da Internet em sua importância social, política e econômica estão repercutindo em novas legislações nacionais que buscam sanar vácuos regulatórios e dirimir conflitos iminentes. Em todos os casos, é possível afirmar que o estabelecimento dessas normatizações quase nunca tem sido pacíficas e são marcadas por tensões entre os interesses de empresas, governos e indivíduos (seja no âmbito do consumo, seja no campo dos direitos). Embates recentes como a guarda de *logs* na aprovação do Marco civil da Internet no Brasil (Lei 12.965/14), a disputa entre a Federal Communications Commission (FCC) e as empresas de telecomunicações nos EUA em torno da neutralidade de rede ou a polêmica na decisão da Corte Europeia de Justiça sobre o “Direito de ser esquecido” na Internet são apenas alguns exemplos neste cenário.

Embora possamos elencar uma série de elementos que estão no fundo dessas disputas, é possível identificar duas preocupações recorrentes que atravessam boa parte desses embates: (a) a concentração de poder dos grandes *players*, principalmente corporações comerciais ou agentes estatais e (b) a proteção de direitos fundamentais dos indivíduos, principalmente quando à liberdade de expressão, direito à livre associação, direito à informação, direito à comunicação e direito à privacidade.

Tendo esta tensão como premissa, a pergunta central que move este *paper* pode ser resumida nos seguintes termos: como está o atual cenário regulatório da Internet e seus principais impactos no direito à privacidade? Mais especificamente, o trabalho se concentra na análise deste tema em três contextos regionais específicos: Brasil, Estados Unidos e União Europeia. A escolha desses três âmbitos se deu em função de

suas respectivas importâncias geopolíticas e por representarem, atualmente, palcos de significativa atividade regulatória nos últimos anos neste campo¹.

Do ponto de vista metodológico, além da revisão de literatura, o estudo se baseou em análise de legislações, normas infralegais, decisões judiciais, diretivas multilaterais, posicionamentos de organizações civis, comerciais e governamentais.

Para responder ao objetivo proposto, o artigo foi organizado em duas seções: primeiro, delinea-se uma compreensão histórica e conceitual da ideia de privacidade, colocando-a no *hall* dos direitos humanos e apontando como este princípio se comporta frente às mudanças trazidas pelas tecnologias digitais de comunicação, especialmente a internet. Com o entendimento conceitual posto, a segunda seção analisará como essas questões estão sendo tratadas nos três contextos políticos em análise (EUA, União Europeia e Brasil), que opções e modelos regulatórios estão sendo configurados; quais os caminhos e impactos sobre o direito à privacidade se desenham nestes cenários.

PRIVACIDADE: DO “DIREITO DE SER DEIXADO SOZINHO” AO “DIREITO DE SER NÃO SER INDEXADO”

Atualmente, qualquer discussão que verse sobre a relação entre direitos e internet passará em algum momento pelo debate sobre privacidade *online*. Um tema complexo, historicamente concebido como um direito individual e que carrega em seu universo semântico questões como autonomia dos sujeitos, mercantilização de informações pessoais, direito ao anonimato, preservação da intimidade. A abrangência deste campo semântico reflete justamente a própria dificuldade em se estabelecer uma definição fechada sobre o que é privacidade, em termos conceituais. Como aponta Solove (2008):

Thus privacy is a fundamental right, essencial for freedom, democracy, psychological well-being, individuality, and creativity. It is proclaimed inviolable but decried as detrimental, antisocial, and even pathological. Some claim that privacy is nearing extinction; others argue that the threat to privacy is illusory. It seems as though everybody is talking about “privacy,” but it is not clear exactly what they are talking about (p. 5).

De tal modo, para termos uma compreensão melhor dos sentidos que hoje preponderam em torno desta questão, precisaremos compreender um pouco da sua trajetória histórica.

Embora rejuvenescida pelos recentes debates sobre proteção de dados e vigilância digital, a concepção jurídica da privacidade enquanto direito tem suas origens no final do século XIX². Ergueu-se nesta época como uma reação à expansão da indústria de mídia impressa (jornais, revistas etc.) que passava a se interessar por informações pessoais (principalmente de personalidades ilustres) como parte de seu repertório de produtos-narrativos (SEVIGANI, 2013; FERNBACK; PAPACHARISSI, 2007; WOO, 2006). O artigo de Samuel Warren e Louis Brandeis, publicado em 1890 pela *Harvard Law Review*, é considerado um dos primeiros documentos que delinea os aspectos centrais da ideia de privacidade como foi concebida desde então. Como explica Woo (2006)

[...] Warren and Brandeis (1890) co-authored a famous article entitled ‘The Right to Privacy’, defining privacy as ‘the right to be let alone’. [...] Warren and Brandeis (1890) argued that news articles and the press invaded people’s private and domestic lives, an argument probably motivated by Warren’s distress at the publicity surrounding his daughter’s wedding (DeCew, 1997) (WOO, 2006, p. 951).

Esse “direito à solidão” deve ser compreendido dentro de um contexto histórico específico: a emergência de uma sociedade liberal que carregava consigo princípios como a universalidade do indivíduo; o temor da ditadura da maioria e do Estado vigilante-opressor; a distinção entre vida pública e vida privada. Ao mesmo tempo, também marca o início do processo de mercantilização de dados pessoais como matéria-prima para indústria da informação. Neste caso, sob a força industrial da *penny press* (TRAQUINA, 2005; BRIGGS; BURKE, 2006) em um cenário de cultura de massa emergente.

Como lembra Solove (2008), praticamente no mesmo período da publicação de Warren e Brandeis, em 1890 Godkin publicou um artigo no qual apontava a privacidade como o direito de decidir o quanto de informações pessoais o público em geral poderia saber de um indivíduo. Embora esta ideia não tenha inicialmente tão influente como a concepção de Warren e Brandeis, isso também evoluiu durante o século seguinte e pode hoje ser vinculada às correntes mais exigentes que veem a privacidade principalmente como uma forma de controle sobre os próprios dados pessoais produzidos.

Atualmente, a ideia de privacidade carrega consigo diferentes questões:

Although the extensive scholarly and judicial writing on privacy has produced many different conceptions of privacy, they can be classified into six general types: (1) the right to be let alone-Samuel Warren and Louis Brandeis’s famous formulation of the right to privacy; (2)

limited access to the self-the ability to shield oneself from unwanted access by others; (3) secrecy-the concealment of certain matters from others; (4) control over personal information-the ability to exercise control over information about oneself; (5) personhood-the protection of one's personality, individuality, and dignity; and (6) intimacy-control over, or limited access to, one's intimate relationships or aspects of life. The conceptions often overlap, but each has a distinctive perspective on privacy. [...] demonstrate that the different conceptions suffer from similar problems. (SOLOVE, 2008, p. 12-13)

Se a concepção moderna de privacidade emerge do “direito de ser deixado sozinho” ou “direito de ter controle sobre a próprios dados” isso não significa que privacidade seja sinônimo de isolamento ou de intimidade. Privacidade trata, mais precisamente, da relação entre intimidade, de um lado, e aquilo que é exógeno, do outro. Ou seja, das fronteiras desta relação. Por isso, a privacidade vai além de um direito calcado na guaranição da vida privada dos olhos do grande público. Consiste em uma questão relacional: trata das trocas entre o “eu” e o “outro, dos limites dessas trocas simbólicas (DeCEW, 1997; WOO, 2006; BUCHMANN et al, 2013). Significa, em outras palavras, afirmar que ao falarmos de privacidade estamos tratando de uma questão social, um fenômeno que está nas bordas das relações entre o indivíduo e aquilo que lhe é externo:

Privacy, however, is not synonymous with the private sphere, but also encompasses the freedom of self-presentation in public whilst maintaining concealment of other aspects of one's self, i.e. there is an inherent tyranny in demanding that any self should totally reveal who they are, and in many contexts anonymity must be safeguarded in public intercourse such as commerce (BUCHMANN et al, 2013, p. 20).

Sendo uma questão social tem seus efeitos políticos. Com o desenvolvimento das democracias modernas percebeu-se que privacidade e autonomia estão umbilicalmente ligadas. Por envolver as fronteiras entre o indivíduo e o que lhe é externo na construção da sua identidade, a privacidade carrega em si uma questão de poder: a autonomia individual só pode ser garantida se os limites dessa intervenção do poder externo (o olhar vigilante de entes potencialmente opressores como público, governos e instituições como a mídia) sobre a intimidade do indivíduo forem devidamente estabelecidos. Por isso, em regimes democráticos, resguardar a autonomia do indivíduo contra esse olhar externo afeta questões centrais que estão na base de um conjunto de direitos e na própria ideia de Estado de Direito, que podemos sintetizar em três conjuntos de questões:

b) Liberdade de escolha e qualidade da participação política - em termos normativos, a participação política só pode ser legitimamente assegurada se for exercida sem

coerção, ou seja, como livre expressão da vontade do indivíduo. A ditadura da maioria pode se manifestar nos casos onde a divulgação de informações privadas coloquem os indivíduos em situações de ataque ou de repressão. Por exemplo, nos caso de sufrágios universais secretos, a privacidade do voto é um direito do eleitor para assegurar que não sofrerá repressão com a divulgação da sua escolha política.

d) Pluralidade de ideias e a livre associação - a privacidade é elemento necessário à promoção da pluralidade democrática, através do compartilhamento privado de opinião entre grupos políticos, culturais e religiosos (garantindo exercício do direito à livre associação). Para que os grupos construam suas identidades coletivas necessitam de privacidade para que possam discuti-las, compreendê-las, adotá-las, defendê-las em público.

c) Preservação da intimidade e Autodeterminação do sujeito - o indivíduo não deve ser refém dos dados privados produzidos que estão sob tutela de forças potencialmente opressoras, seja no nível comercial quanto governamental. Ou seja, para se garantir a autonomia do sujeito é preciso estabelecer as fronteiras entre esse poder externo e o *self*). (BUCHMANN et al, 2013; PHILLIPS, 2004)

É justamente por se tratar de uma questão relacional com fortes impactos na dimensão social e política que a privacidade envolve processos de comunicação. O presente cenário de inovações tecnológicas afeta cada uma dessas dimensões elencadas. De forma mais sintética, Phillips (2004) aponta quatro ênfases que se erguem nas preocupações com privacidade em sua relação com as novas tecnologias: (1) proteção contra intrusão; (2) negociação entre o público e o privado; (3) gerenciamento de identidade e (4) proteção contra vigilância. Não por acaso, fenômenos tecnológicos-sociais como a “datificação” da vida contemporânea (MAYER-SCHONBERER; CUKIER, 2013; LESSING, 2004) afetam diretamente a privacidade pois alteram as bases da produção, coleta e circulação de informação pessoal. Em um contexto de crescente poder das corporações que tem em suas mãos um enorme volume de dados pessoais digitalizados:

[...] the accumulated power of Internet corporations (financial, network-making, discursive) enable Internet privacy crises that are driven by surveillance-based business models. Privacy is either declared to be obstructive or it must take the form of a commodity to fit into the corporate Internet. The latter implies that personal data are perceived as private property that is exchangeable for certain benefits (SEVIGNANI, 2013, p. 735).

A mercantilização de informação pessoal pela indústria da informação não é algo novo: como vimos, isso já era feito pelo *mass media* no final do século XIX. Porém, em tempos de Internet, o foco não é a mais obtenção de dados pessoais para ser publicado e consumido como um produto-narrativo midiático. A ênfase atualmente é distinta: os dados pessoais se transformaram em *commodities* (valorizadas sob o título de informação estratégica valiosa para outras corporações) que são obtidas pelas empresas através da cessão voluntária de dados pessoais por um benefício básico: o uso da ferramenta. Na prática, o cidadão abre mão da sua privacidade em troca do próprio acesso à plataforma, gerenciadas em sua maioria por grandes corporações privadas (PHILLIPS, 2004; WOO, 2006). Até porque não lhe restaria mais do que duas opções simples: ou aceita-se os termos de privacidade colocados pelo serviço ou não se pode utilizá-lo.

Paradoxalmente, ao mesmo tempo que há uma crescente valorização dos dados pessoais como *commodity* no mercado (Phillips, 2004) há também uma tendência de desvalorização da noção de privacidade como direito individual, uma vez que seu valor de troca se nivela ao simples uso do produto.

Além da “barganha” (ou da simples troca da privacidade pelo uso da ferramenta) as empresas também tem buscado convencer os usuários em ceder seus dados pessoais sob a justificativa de obter uma melhor experiência com o serviço:

The discourse about cookies is framed in terms of convenience to the user; deleting them will result in a less streamlined, less personal and less productive MSN web experience. This statement also serves, rhetorically, to comfort the user that cookies are not dangerous (i.e. they do not deliver viruses), although they are used to monitor consumer online activity (Lipschultz, 2001). Whatever privacy concerns might be raised by the notion that monitoring devices are placed on the user's computer are mollified discursively by the emphasis on convenience. Thus the consumer is positioned to make a choice between privacy and convenience (FERNBACK; PAPACHARISSI, 2007, p. 724).

Para Woo (2006) a sujeição voluntária à vigilância não parece constituir um “invasão” do espaço pessoal por forças externas a ponto de violar o “*right to be alone*”. Por isso, para o autor, conceito tradicional de privacidade - baseado na invasão unilateral do espaço pessoal por forças externas - e a subsequente produção de políticas com esta visão - não funcionam mais neste cenário. Ele explica que a autonomia do indivíduo, neste contexto de poderosas e onipresentes tecnologias digitais de monitoramento, só poderia ser garantida se passarmos a compreender a noção de privacidade não mais como o “direito de ser deixado sozinho” e sim como o “direito de não ser identificado”.

Paralelamente, isso não significa que isso resolve o problema conceitual do que deveríamos compreender por privacidade. Para Solove (2008) todas as definições e ênfases que foram somadas nesta trajetória do termo falham por serem demasiadamente amplas, vagas ou estritas. Por isso, o autor acredita que:

A theory of privacy should focus on the problems that create a desire for privacy. Privacy concerns and protections do not exist for their own sake; they exist because they have been provoked by particular problems. Privacy protections are responses to problems caused by friction in society. [...] privacy by focusing on the specific types of disruption and the specific activities disrupted rather than looking for the common denominator that links all of them. Privacy protections address a web of interconnected problems that disrupt specific activities (SOLOVE, 2008, p. 76-77).

Tendo em vista esta característica multidimensional e que envolve diversos problemas de natureza individual e social e, diante disso, observando o crescimento do poder de diversos *players* neste campo nos últimos anos (principalmente empresas que lidam com comunicação digital), Fernback e Papacharissi (2007) defendem que a privacidade seja tratada mais devidamente como bem público:

Because privacy encompasses both social and economic dimensions, the concept of privacy itself can be regarded as a public good. Public goods such as parks, postal services or universal education contribute to the well-being of a society without any determinable material price, value, ownership or structure for compensation [...] Therefore, conceiving of privacy as a public good is a useful foundation for providing recommendations for a democratic internet privacy policy (p. 731).

Olhar a privacidade como bem público parece razoável e requer priorizar padrões regulatórios com base em princípios normativos bem delimitados e concretos. Ao mesmo tempo, isso requer levar em conta pensar a noção de privacidade para além do foco no indivíduo. Como aponta Poritz (2007), em geral as leis vigentes reconhecem algum nível de proteção à privacidade individual (em diferentes graus e ênfases), mas poucas versam de fato sobre a privacidade coletiva.

No mundo, há hoje um intenso debate sobre os modelos e caminhos regulatórios para a privacidade no ambiente digital. Porém, ainda há pouca regulação específica recentemente consolidada salvaguardando direitos. Em muitos contextos, ainda não há ainda um efetivo controle das empresas sobre o uso comercial de dados pessoais.

PRIVACIDADE *ONLINE* E REGULAÇÃO NOS EUA, UNIÃO EUROPEIA E BRASIL

O processo de regulação da comunicação digital vem se configurando, desde o início deste século, através de diferentes formatos e graus de abrangência. Algumas normas têm sido pactuadas em acordos internacionais, principalmente em torno de organizações multilaterais. Outras, são objeto natural da legislação de um ente nacional, de uma comunidade supranacional ou de um ente federativo, principalmente no que se refere àqueles vinculados a questões práticas, como comércio e violação de direitos.

Com as bases conceituais delineadas na seção anterior, neste momento passaremos a observar como a privacidade *online* está sendo tratada em cada um dos três contextos em estudo: EUA, União Europeia e Brasil. A análise ocorrerá buscando identificar qual o *background* legal que prevalece em cada realidade e quais os modelos regulatórios que vem se configurando em torno deste direito, sobretudo diante das novas possibilidades e atritos gerados pela expansão do uso cotidiano da comunicação *online*.

MODELOS REGULATÓRIOS

Nos EUA, há hoje quatro principais leis que tratam da privacidade e proteção de dados pessoais frente às corporações: (1) o *Children's Online Privacy Protection Act* (COPPA) de 1998; (2) o *Telecommunications Act de 1996*; o (3) *Health Insurance Portability and Accountability Act* (HIPAA) de 1996; e o (4) *Gramm-Leach-Bliley Act* (GLB) de 19993.

A GLB diz respeito principalmente a informações financeiras. A HIPAA lida com as regras sobre o armazenamento de dados de identificação como nome, idade, número de telefone, número de seguridade social etc. Nestes dois casos, ambas as leis dedicam apenas trechos delimitados para tratar de privacidade. No caso do *Telecommunications Act* têm-se importantes parágrafos sobre as obrigações de privacidade dos operadores da rede, dos *common carriers*. Por fim, a normatização mais concentrada no tema privacidade é a COPPA que dita as normas e proibições sobre coleção e disseminação de informação pessoal sobre crianças de até 13 anos. Nota-se que o país ainda não possui uma lei específica sobre privacidade digital. O principal ente regulador de temas que envolvem dados pessoais e privacidade frente às empresas é a *Federal Trade Commission* (FTC): uma agência federal de proteção ao consumidor e de políticas de competição de mercado.

No caso estadunidense, prevalece um modelo de regulação caracterizado pelo pouco rigor no controle de possíveis violações. Os princípios são geralmente vagos e o ente regulador tem baixa intervenção. O que coloca as empresas comerciais em uma posição confortável para lidar com os dados pessoais produzidos pelos indivíduos *online*:

The privacy statement formula follows in the tradition of self-regulation prevalent in the USA, which is founded on a lack of government involvement in regulating consumer privacy (with the exception of the Children's Online Privacy Protection Act of 1998 (COPPA)). The adequacy of privacy statements as protective measures is arguable; attorneys frequently draft online privacy statements to include catch-all stipulations that permit flexibility regarding uses of consumer information (Fausett, 2001) (FERNBACK; PAPACHARISSI, 2007, p. 719).

Isso tem resultado em um cenário de pouca proteção à privacidade na prática. Por exemplo, Fernback e Papacharissi (2007) apontam que um estudo da FTC revelou que apenas 20 % dos *websites* estadunidenses haviam implementado as diretrizes da Agência para práticas informacionais adequadas. Como sintetiza Phillips (2004):

In summary, these rules permit data-holders to do anything they want with information derived from and produced by individuals, provided that they de-link the data from the individual's indexical identity. The actions of individuals may be used to describe and model them in any way that the data-holder wishes, provided the data-holder cannot actually contact, locate, point to or act upon the individual thus described. They are, again, informed by an understanding of 'privacy' that is closely related to the protection of the individual from unwanted intrusion (p. 701).

Atualmente, há projetos de lei sobre privacidade no Congresso americano, como *Online Personal Privacy Act* ou ainda propostas de leis que abordam privacidade e vigilância, como o *Cybersecurity Information Sharing Act (CISA)* e *Cyber Threat Sharing Act*. Porém, todos sem avanço efetivo na tramitação. Para alguns analistas, os EUA permanecem como "the only major trading nation which has not adopted comprehensive privacy protection legislation" (FERNBACK; PAPACHARISSI, 2007, p. 719).

No caso europeu, a União Europeia estabelece normas comuns que tentam amarrar todos os países do bloco com diretivas a serem implementadas por cada estado membro (FRA, 2014). As duas principais diretivas europeias sobre privacidade são o *Data Protection Directive*, aprovada em 1995 e em vigor desde 1998 (que é atualmente a principal norma, também conhecida como *Directive 95/46/EC*⁴) e a *Directive on Privacy and Electronic Communications*, de 2002 (também conhecida como o "Telecoms Package", por lidar com o setor de telecomunicações e, dentro disso, traz algumas direções sobre privacidade).

Em geral, os países europeus possuem leis mais rígidas quanto à privacidade, destoando do modelo que prevalece nos EUA. Ao contrário do caso americano, a legislação europeia dá maior atenção à proteção da privacidade de consumidores e as agências reguladoras agem de modo mais incisivo neste campo (FERNBACK; PAPACHARISSI, 2007; BUCHMANN et al, 2013; BYGRAVE, 2015). Porém, embora seja considerada mais rígida do que o padrão norte-americano, a principal legislação que trata deste tema, a *Directive 95/46/EC*, também tem suas fragilidades, principalmente porque não consegue prever de forma efetiva o cenário de convergência digital e, além disso, por não ser uma regulação completa na forma de lei (e sim uma diretiva) possui falhas em uniformizar o modo como todos os países da comunidade agem sobre o tema. Como explica Costa e Pouillet (2012):

The harmonization obtained by the Directive 95/46 has seemed insufficient. The strong reassertion of the Data Protection as a fundamental right, both by the article 8 (1) of the 2000 EU Charter of fundamental rights and by the article 16 (1) of the Treaty, requires an effective and more coherent protection of the EU citizens throughout the European Union. It might be added that due to the increasing number of data flows and their globalization, Europe might no longer accept different national data protection legislations both as regards their content and their effectiveness (p. 254).

Embora possamos falar de uma perspectiva europeia mais rígida quando comparada ao modelo estadunidense em linhas gerais, isso não significa que todos os 28 membros da UE estão totalmente distantes do modo norte-americano ou que haja uma coesa ação regulatória neste sentido entre esses países. Na prática, é possível encontrar, no nível nacional, práticas mais formais ou menos formais na aplicabilidade dessas normas, em alguns casos se aproximando da perspectiva norte-americana na prática, como explica Bamberger e Mulligan:

Despite the divergence between Germany and the United States regarding both the language in which privacy is discussed and the particular mandates and institutions shaping privacy's governance, the architecture for privacy protection and decision making within German firms bears considerable resemblance to the emerging best practices we identified in the United States—practices that reveal particular adaptability and suitability for addressing new challenges of the digital age. By contrast, the privacy models in Spain and France differ from the U.S. structure, focusing on more formal data registration, use, and reporting requirements. This focus appears to position expertise outside the firm, with the formal regulators, decreasing investment in internal privacy expertise and limiting the reach and power of internal privacy experts. (2013, 1537-1538)

Por isso, em janeiro de 2012 a Comissão Europeia lançou uma proposta de marco regulatório sobre proteção de dados pessoais chamado *General Data Protection Regulation*. Trata-se de um projeto de lei que visa substituir a Directive 95/46 e alinhar o tema em todos os estados-membros. Para a Comissão Europeia:

Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe⁵.

O projeto ainda está em debate sendo considerado uma questão prioritária em 2015. Ao finalizar a proposta, a Comissão ainda enviará para o Conselho e para o Parlamento Europeu que poderão aprovar ou propor alterações.

Já no caso brasileiro, até o início desta década, a legislação sobre privacidade basicamente se resumia a alguns artigos da Constituição Federal de 1988 e do Código Civil (Lei nº 10.406, de 2002.). Com a inexistência de uma lei específica, os litígios sobre invasão de privacidade e proteção de dados *online* vinham sendo resolvidos através de jurisprudência. Ou seja, a Justiça acabava gerando decisões com base na escassa normatização e essas sentenças se tornavam parâmetros para julgamentos futuros.

Neste cenário, alguns Projetos de Leis que versavam sobre privacidade e crimes cibernéticos surgiram no Congresso Nacional. Em 2012, foi aprovada a Lei nº 12.737 (também conhecida como lei Carolina Dieckmann) que trata de invasão de dados pessoais e, indiretamente, lida com privacidade (embora a palavra “privacidade” não apareça no texto. Também surgiram outras proposições, como o Projeto de Lei 84/1999, de autoria do deputado federal Eduardo Azeredo chegou a ser aprovado na Comissão de Ciência e Tecnologia da Câmara em 2012, mas recebeu um conjunto de críticas por tratar o usuário *online* predominantemente do ponto de vista criminal sem respeitar liberdades e direitos individuais. Acabou não tendo sua tramitação avançada.

Em meio a esse vácuo jurídico, o Ministério da Justiça lançou em 2009 o projeto do *Marco Civil da Internet*: uma consulta pública para uma futura lei que versaria sobre os direitos civis dos cidadãos *online*, incluindo uma seção sobre privacidade digital. A Lei 12.965 foi aprovada em abril de 2014 e está desde então em processo de implementação.

É possível afirmar que a lei do Marco Civil trouxe avanços importantes sobre a privacidade *online* e estabelece algumas normas na relação entre consumidor e provedores, diminuindo assim a insegurança jurídica até então vigente. Porém, há algumas limitações relevantes nesta nova legislação que ainda precisariam ser superadas: (a) a lei está em processo de regulamentação de artigos importantes por isso ainda necessita de normas complementares para funcionar de fato; (b) a lei não trata de privacidade de modo mais abrangente e, por isso, será complementada por uma outra legislação específica sobre proteção de dados, ainda em processo de elaboração⁶; (d) permanece a lacuna do ente regulador para o tema, um reflexo das fragilidades do sistema regulatório no país.

Além desses obstáculos, a forma como a guarda de *logs* foi definida pela lei também tem sido objeto de críticas. A nova norma passou a exigir a manutenção compulsória de dados de conexão do usuário para “eventuais investigações” sob ordem judicial por um período de 12 meses no caso dos provedores de acesso e durante 6 meses no caso dos provedores de aplicações. Embora a norma deixe clara a inviolabilidade das informações e obrigue as empresas a mantê-las seguras, para algumas organizações e ativistas, esta determinação consiste em uma forma de “grampo” prévio a todo cidadão. Ou seja, na prática cada indivíduo passa a ser indiscriminadamente monitorado, invertendo o princípio constitucional da presunção de inocência⁷. As críticas também afirmam que não há garantias de que os provedores possam utilizar comercialmente os dados pessoais dos usuários a fim de amortizar os custos de manutenção desses registros.

TENDÊNCIAS NO CAMPO JURÍDICO

Como vimos, embora tenhamos uma regulação mais solta nos EUA, um pouco mais configurada na Europa e em implementação no Brasil, em todos os casos há muitas lacunas jurídicas onde a própria concepção de privacidade não está devidamente definida. Isso leva diversos casos para as cortes e, no âmbito jurídico, também podemos visualizar tendências, principalmente quando a jurisprudência age sobre as lacunas e aponta visões sobre os limites do direito à privacidade em tempos de intensos fluxos de dados digitais. Neste sentido, aquilo que vem sendo chamado de “*O Direito de ser esquecido*” serve como um bom parâmetro, principalmente porque envolve questões conceituais sobre as fronteiras do direito à privacidade frente aos interesses dos grandes players e os desafios que as tecnologias digitais impõem neste cenário.

Embora seja nomeado de “Direito de ser esquecido” este tema ainda não se consolida como um direito em *strictu sensu*: trata-se ainda de um debate sobre o potencial direito de não ser identificado *online*, de não ser indexado pelas plataformas digitais sob a justificativa de que isso violaria o princípio da privacidade ou, mais especificamente, a ideia de privacidade como controle do cidadão sobre os dados pessoais que produz:

The right to informational self-determination lies at the root of the right to be forgotten. Based on the fundamental principles of dignity and self-development, the right to informational self-determination “provides individuals the power to decide themselves about issues of collection, disclosure and use of their personal data” (COSTA e POULLET, 2012, p. 257).

Na Europa, o tema chegou aos tribunais primeiramente com o caso de um advogado espanhol, Mario Costeja Gonzáles, que foi obrigado a vender alguns de seus bens em processos de insolvência no final 1990. Um jornal espanhol (La Vanguardia) reportou sobre o processo na época. Gonzáles resolveu seus problemas financeiros. Porém, quando o jornal passou a disponibilizar toda sua base de conteúdo na Internet, as informações sobre o problema financeiro de Gonzáles se tornaram acessíveis para um grande público. Diante disso, em 2010, o espanhol pediu que o La Vanguardia removesse as informações e o Google retirasse os resultados para a busca com seu nome. A Agência Espanhola de Proteção de dados julgou o caso e considerou que o La Vanguardia não precisaria retirar o conteúdo publicado *online*, mas o Google foi obrigado a apagar do seu buscador o tema sobre a insolvência financeira do advogado espanhol. O caso foi parar na Corte Europeia de Justiça que confirmou a validade da decisão da Agência.

A decisão tem gerado polêmica tanto na Europa quanto do outro lado do Atlântico e demonstra claramente uma tendência europeia de maior rigidez com a proteção da privacidade. Nos EUA, o New York Times publicou editorial criticando a decisão e apontando seus eventuais efeitos sobre o direito à informação:

The European position is deeply troubling because it could lead to censorship by public officials who want to whitewash the past. It also sets a terrible example for officials in other countries who might also want to demand that Internet companies remove links they don't like⁸.

Para Toobin (2014) a decisão também demonstra que o modelo europeu estaria priorizando a privacidade em detrimento da liberdade de expressão e que o modelo americano faria justamente o inverso. O autor explica que nos EUA já houve ação semelhante no Texas, por exemplo, mas que a Justiça deu ganho de causa para o Google. Ele acredita

que “the American regard for freedom of speech, reflected in the First Amendment, guarantees that the Costeja [Gonzalez] judgment would never pass muster under U.S. law” (2014, *online*)

A tendência europeia, neste caso, também parece não fazer coro no Brasil. A nova lei brasileira sobre o tema (Marco Civil da Internet) não versa sobre o papel dos buscadores no “direito de não ser indexado”. Em linhas gerais, estipula que a retirada de conteúdo *online* só pode ser feita por ordem judicial. Em casos que afetam a privacidade e intimidade, a lei também prevê a possibilidade do indivíduo atingido negociar a retirada diretamente com a empresa. A jurisprudência que tem prevalecido no país diverge da posição europeia. Em 2012 o Supremo Tribunal de Justiça (STJ) não acatou o pedido da apresentadora Xuxa Meneghel para que o Google retirasse os resultados de busca para termos como “Xuxa pedófila”⁹. Em 2014, o caso chegou ao Supremo Tribunal Federal (STF) que manteve a decisão do STJ. E assim, outros tribunais regionais tem seguido este mesmo posicionamento para casos similares¹⁰.

CONCLUSÃO

Este artigo teve como objetivo compreender o atual estágio de regulação da comunicação digital e seus impactos no direito à privacidade, especificamente no âmbito de três contextos geopolíticos: Brasil, EUA e União Europeia.

O estudo buscou configurar primeiramente uma compreensão do direito à privacidade, partindo histórica e conceitual do termo. A análise demonstrou que o termo tem uma história relativamente recente no campo dos direitos, sendo de fato desenvolvida somente a partir do século XIX, principalmente sob forte influência da concepção de privacidade enquanto “direito de ser deixado sozinho”. A partir daí uma série de outras concepções e ênfases foram sendo acopladas, deixando o termo demasiadamente vago em muitos casos e atualmente ainda carente de uma conceituação mais clara, concreta e aplicável.

Do ponto de vista regulatório, os resultados demonstram que há atualmente modelos regulatórios distintos nos contextos analisados. Nos EUA prevalece uma regulação fraca marcada pelo *laissez-faire* e empoderamento das empresas sobre os dados pessoais *online*. No caso brasileiro, a regulação recém aprovada traz avanços (como a proibição do comércio de dados pessoais; regras e obrigações na guarda de dados etc.) mas

ainda está em processo de regulamentação e implementação. Já na Europa, o cenário é marcado por um conjunto de realidades legislativas e jurídicas tradicionalmente mais comprometidas com o princípio da privacidade, havendo assim um quadro regulatório mais denso quanto a este tema. Porém, em todos os três casos, há lacunas legislativas e algum nível de insegurança jurídica, o que tem levado o tema para disputas em tribunais e cortes superiores. No nível jurídico, Brasil e EUA tem adotado uma visão de privacidade menos radical quanto ao empoderamento do indivíduo no controle dos dados pessoais *online* enquanto a corte europeia tem levado a cabo a ideia do *direito de não ser indexado*.

Todo esse quadro demonstra que a regulação da Internet é um processo que já está em andamento e, devido à sua complexidade, ocorre em velocidades distintas e em graus de desenvolvimento diferentes entre os países. No atual estágio regulatório, nota-se que há ainda escassas legislações específicas que tratem da proteção dos direitos civis na Internet. Essas poucas leis, como o Marco Civil brasileiro, foram aprovadas recentemente e encontram-se nos primórdios de suas implementações e suas efetivações ainda precisam ser colocadas à prova.

REFERÊNCIAS

BAMBERGER, Kenneth A.; MULLIGAN, Deirdre K.. Privacy in Europe: Initial Data on Governance Choices and Corporate Practices. *The George Washington Law Review*, 81(5), p. 1529-1664, 2013.

BEREC. Body of European Regulators for Electronic Communications. **Summary of BEREC positions on net neutrality**. BoR (12) 146, 2014. Disponível em <http://berec.europa.eu/files/document_register_store/2012/12/BoR_%2812%29_146_Summary_of_BEREC_positions_on_net_neutrality2.pdf> Acesso 18 de janeiro 2015.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Disponível em: <www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso: 10 ago. 2013.

BRASIL. **Lei Nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso: 10 jan. 2015.

BRASIL. **Lei Nº 10.406**, de 10 de janeiro de 2002 (Código Civil Brasileiro). Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso: 16 jan. 2015.

BRIGGS, Asa & BURKE, Peter. **Uma história social da mídia: de Gutemberg à Internet**. Rio de Janeiro: Jorge Zahar Editor, 2006.

BUCHMANN, Johannes et al. **Internet Privacy: Options for adequate realisation**. Berlin: Springer-Verlag Berlin Heidelberg, 2013.

BYGRAVE, Lee A. Law and Technology A Right to Be Forgotten? **Communications Of The ACM**, 58(1), p. 35-37, 2015.

CLARK, David D. **An Insider's Guide to the Internet**. MIT Computer Science and Artificial Intelligence Laboratory (Version 2.0). Cambridge: MIT, 2004

COOPER, Alissa. **How Regulation and Competition Influence Discrimination in Broadband Traffic Management: A Comparative Study of Net Neutrality in the United States and the United Kingdom**. 2013. Tese de doutorado (Doutorado em Communication and the Social Sciences). University of Oxford, St. Catherine's College.

COSTA, Luiz; POULLET, Yves. Privacy and the regulation of 2012. **Computer Law & Security Review**, p. 254-262, 2012

DeCEW, Judith W. **In Pursuit of Privacy: Law, Ethics, and the Rise of Technology**. Ithaca e Londres: Cornell University Press, 1997.

EUA. Estados Unidos da America. **Telecommunications Act** de 1996. Disponível em <<http://transition.fcc.gov/Reports/tcom1996.pdf> >

EUA. Estados Unidos da América. **HIPAA - Health Insurance Portability and Accountability Act** de 1996. Disponível em <<http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf> > acesso 14 novembro 2014.

EUA. Estados Unidos da America. **COPPA - Children's Online Privacy Protection Act** de 1998. Disponível em <<https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>> acesso 13 novembro 2014.

EUA. Estados Unidos da América. **GLB - Gramm-Leach-Bliley Act** de 1999. Disponível em < <http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf> > acesso 14 novembro 2014.

FERNBACK, Jan; PAPACHARISSI, Zizi. Online privacy as legal safeguard: the relationship among consumer, online portal, and privacy policies. **New Media & Society**, 9(5), p. 715-734, 2007.

FRA. European Union Agency for Fundamental Rights. **Handbook on European data protection law**. Luxembourg: Publications Office of the European Union, 2014. Disponível em <<http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law> >. Acesso 4 de fevereiro 2015.

LESSING, Lawrence. **Free Culture: how big media uses technology and the law to lock down culture and control creativity**. Nova York: The Penguin Press, 2004.

LESSIG, Lawrence; MCCHESENE Y, Robert W. No Tolls on the Internet. In: **Washington Post**. 8 de junho de 2006. Disponível em <<http://www.washingtonpost.com/wpdyn/content/article/2006/06/07/AR2006060702108.html>>. Acesso em: 27 jun. 2012.

MARCUS, Scott. **Network Neutrality Revisited: Challenges and Responses in the EU and in the US**. Bruxelas: Parlamento Europeu, 2014. Disponível em <http://www.europarl.europa.eu/RegData/etudes/STUD/2014/518751/IPOL_STU%282014%29518751_EN.pdf> .

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big Data: A Revolution That Will Transform How We Live, Work, and Think**. Nova York: HMHBooks, 2013

OLMOS, Ana; CASTRO, Jorge. **Net Neutrality in the EU - Country Factsheets (Report)**. Brussel: Open Forum Academy, 2013. Disponível em <<http://www.openforumacademy.org/library/ofa-research/OFA%20Net%20Neutrality%20in%20the%20EU%20-%20Country%20Factsheets%2020130905.pdf>> .

PHILLIPS, David J. Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. **New Media & Society**, 6(6), p. 691-706, 2004

PORITZ, J. Who searches the searchers? Community privacy in the age of monolithic search engines. **Information Society**, 23 (5), p. 383-89, 2007.

SEVIGNANI, Sebastian. The commodification of privacy on the Internet. **Science and Public Policy**, 40, p. 733-739, 2013.

SHELANSKI, Howard A. Network Neutrality: regulating with more questions than answers. **Journal on Telecommunications and High Technology Law**, 6, p. 23-40, 2007.

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

TOOBIN, Jeffrey. The Solace of Oblivion: In Europe, the right to be forgotten trumps the Internet. **Annals of Law - New Yorker**, 29, 2014 (online). Disponível em <<http://www.newyorker.com/magazine/2014/09/29/solace-oblivion>> .

TRAQUINA, Nelson. **Teorias do Jornalismo: porque as notícias são como são (vol I e II)**. Florianópolis: Insular, 2005.

UE. União Europeia. **Data Protection Directive - Directive 95/46/EC of the European Parliament and of the Council** de 24 de outubro de 1995. Disponível em <<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>> acesso 11 novembro 2014.

UE. União Europeia. **Directive on Privacy and Electronic Communications - Directive 2002/58/EC of the European Parliament and of the Council**, de 2002. Disponível em <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML>> acesso 9 novembro 2014.

WOO, Jisuk. The right not to be identified: privacy and anonymity in the interactive media environment. *New Media & Society*, 8(6), p. 949-967, 2006.

NOTAS

1. Os EUA por serem o berço da Internet, a maior economia em atividade e um dos mais importantes e influentes centros de produção de tecnologia. O Brasil por ser o maior país da América Latina, com o quarto maior contingente de usuários de Internet (conforme dados da União Internacional de Telecomunicações) e que aprovou recentemente o Marco Civil da Internet (considerado por especialistas e organizações como uma importante legislação nacional que trata especificamente dos direitos civis *online*). E a União Europeia também pela importância e influência econômica e tecnológica, que soma um grande contingente de usuários. Embora esta última não seja necessariamente um país como os outros dois casos e sim um sistema de instituições supranacionais independentes, temas como a privacidade são guiadas por diretivas das quais todos os estados-membros devem seguir, principalmente quanto aos objetivos estipulados (ainda que a forma e meios para atingir esses objetivos sejam flexíveis no nível nacional).
2. É possível traçarmos toda uma discussão sobre a dicotomia entre o “público” e o “privado” desde a antiguidade, passando pela Idade Média até chegar no debate iluminista. Estas concepções sofreram diversas mutações na História. Porém o “Privado” não é o mesmo que “privacidade”, ainda que tenham suas intersecções etimológicas. A ideia da “privacidade” enquanto um direito individual que começa a ganhar contornos mais definidos no âmbito legal ocorre somente a partir do século XIX.
3. Em outro campo de análise, isto é, na regulação da privacidade do indivíduo frente ao Estado existem o Privacy Act de 1974 e também o Patriot Act of 2001.
4. Disponível em < <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=en> > Acesso 8 de junho de 2015.
5. Ver em < http://ec.europa.eu/justice/data-protection/reform/index_en.htm >. Acesso 25 setembro 2015.
6. Em paralelo à consulta pública para regulamentar os artigos do Marco Civil, o Ministério da Justiça também abriu uma debate para elaboração da minuta do Projeto de Lei de Proteção dos Dados Pessoais. Este texto visa ir além de questões de privacidade na Internet e tratará, por exemplo, da proteção da privacidade junto a bancos, empresas telefônicas, seguradoras etc..
7. Ver texto integral da carta em < <http://marcocivil.org.br/cartamc/> > Acesso 5 mar 2015.
8. O texto na íntegra está disponível em <:http://www.nytimes.com/2015/02/04/opinion/europes-expanding-right-to-be-forgotten.html?_r=0 > acesso 4 fevereiro 2015.
9. Veja íntegra da decisão no *site* do Superior Tribunal de Justiça <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201103079096&dt_publicacao=29/06/2012 >
10. Como o caso da decisão do Tribunal de Justiça de Goiás: < www.conjur.com.br/2015-fev-19/google-nao-obrigado-excluir-nomes-sistema-busca-tj-go >

Artigo recebido: 30 de outubro de 2015

Artigo aceito: 02 de dezembro de 2015