Artigos Selecionados REDE 2017
I Encontro da Rede de Pesquisa em Governança da Internet
Rio de Janeiro, 14 de Novembro de 2017

PROTEÇÃO DE DADOS PESSOAIS COMO REGULAÇÃO DE RISCO: uma nova moldura teórica?[1]

Rafael A. F. Zanatta
Doutorando pelo Instituto de Energia e Ambiente da Universidade de São Paulo.
Mestre em Direito pela Universidade de São Paulo.
Mestre em Direito e Economia pela Política pela Universidade de Turim.
rafaelzanatta@usp.br

RESUMO

A proteção de dados pessoais, enquanto campo de afirmação de direitos e regulação do comportamento público e privado relacionados aos processos de coleta e análise de informações pessoais, tem passado por intensas transformações. Na União Europeia, com o advento do *General Data Protection Regulation* que entra em vigor em 2018, diversos autores falam da emergência da "risquificação" da proteção de dados pessoais e uma mudança de emolduramento teórico dos direitos deste campo, especialmente com o advento de instrumentos de regulação *ex ante* direcionados à mitigação a "danos coletivos" e ameaças a liberdades fundamentais. O presente artigo analisa o significado do processo de risquificação da proteção de dados pessoais e os principais argumentos mobilizados pelos autores que defendem a existência desse fenômeno. Considerando que a discussão é pouco conhecida na literatura brasileira de ciências sociais e governança da internet, o artigo explica, de forma sintética, diferentes abordagens teóricas sobre proteção de dados pessoais. Na sequência, discute-se o conjunto de transformações jurídicas e institucionais rotuladas como "risquificação", especialmente no contexto europeu. Por fim, o artigo busca evidencias da existência desse fenômeno no processo de construção legislativa de proteção de dados pessoais no Brasil e identifica perguntas que poderiam compor a agenda de risquificação no Brasil.

PALAVRAS-CHAVE: proteção de dados pessoais, regulação do risco, risquificação, direito regulatório;

---

1 O presente artigo foi apresentado no "I Encontro da Rede de Governança da Internet", em novembro de 2017, no Rio de Janeiro, e se beneficiou das discussões e apontamentos feitos por Bruno Bioni, Danilo Doneda, Diego Canabarro, Renato Leite Monteiro, Ricardo Abramovay e os participantes do seminário. Erros e imprecisões são de minha responsabilidade.

Sugestão de citação (ABNT): SOBRENOME, Nome. **Título do artigo**. I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, NOVEMBRO DE 2017. Disponível em: <endereço na web>. Acesso em: mês. ano.

INTRODUÇÃO

Há quase meia década, os professores Serge Gutwirth e Yves Poullet apontaram que "a proteção de dados pessoais estava em um ponto de virada" e em um "renascimento" (GUTWIRTH e POULLET, 2013). Eles se referiam ao longo processo de elaboração e aprovação do *General Data Protection Regulation* (GDPR), considerada por alguns acadêmicos como a legislação mais avançada para proteção dos "titulares de dados pessoais" no mundo (DE HERT e PAPAKONSTANTINOU, 2012). Dentre as diversas mudanças observadas na legislação europeia – que tem causado um certo *frisson* no circuito de tecnologia pelo seu caráter extraterritorial – e seu significado para o direito como um todo, pesquisadores do campo jurídico apontam para um processo em específico: a *"risquificação" do direito*, onde a afirmação de direitos fundamentais é complementada por uma preocupação maior com instrumentos de regulação *ex ante,* licenças, análises de risco, processos de documentação e *accountability* por parte dos "controladores" e "processadores" de dados (GELLERT, 2015; QUELLE, 2015; SPINA, 2017). O presente artigo aprofunda-se nessa questão para explicar o que consiste a guinada teórica para regulação do risco na proteção de dados pessoais e sua relevância para uma reproblematização, em nível intelectual e político, dos arranjos de proteção de dados pessoais no Brasil.[2]

Para compreensão do processo de risquificação e a crescente importância da "regulação do risco", é preciso analisar o modelo teórico dominante na segunda metade do século XX, período em que surgiram as normas jurídicas de proteção de dados pessoais.[3] Em termos tipológicos, contrastarei o modelo teórico da autodeterminação informacional com o modelo da regulação do risco.[4]

---

2 Por "guinada teórica" quero designar o processo de incorporação de novas lentes de análise ao debate sobre proteção de dados pessoais e não um processo de colisão jurídica ou substituição normativa. Não defendo, no plano normativo, a substituição da matriz de direitos fundamentais por uma matriz de "regulação baseada no risco". Como observado por acadêmicos da área (GELLERT, 2015; QUELLE, 2015), a adoção da "linguagem do risco" também pode, se utilizada de forma inadequada, fragilizar a proteção de direitos fundamentais.

3 Não é objetivo desse artigo realizar uma extensa análise histórica sobre o desenvolvimento do direito à proteção de dados pessoais e as raízes no direito à privacidade. Para estudos nesse sentido, ver Doneda (2006) e Mendes (2014).

4 Alguns leitores poderão reagir contrariamente a essa proposta, alegando que já havia elementos de mitigação de riscos no direito da proteção de dados pessoais construído no século XX. Conforme explicado nas notas 13 e 15, não se trata de comparação de normas jurídicas existentes ou de "gerações de normas", mas de discussão de modelos teóricos (um dominante e outro emergente), construídos como instrumentos heurísticos.

1. PROTEÇÃO DE DADOS PESSOAIS: DA AUTODETERMINAÇÃO INFORMACIONAL À REGULAÇÃO DE RISCO

A literatura brasileira possui uma boa discussão sobre a formação teórica da proteção de dados pessoais no século XX. Danilo Doneda, em tese de doutorado que definiu os termos do debate nacional em 2006, afirma que o desenvolvimento do *direito à proteção de dados pessoais* incorpora alguns elementos do debate estadunidense sobre controle e autonomia individual – originários do *privacy law*, com sua construção casuística e posterior construção estatutária em nível federal –, mas se torna mais complexo ao envolver uma concepção de tutela (proteção jurídica) enquanto elemento basilar de liberdades democráticas, ressignificando a proteção dos direitos da personalidade a partir de uma matriz westiniana[5] de autonomia e "controle das informações pessoais". Para Doneda, a proteção de dados pessoais transforma a concepção contemporânea de proteção da privacidade, deixando de "dar vazão somente a um imperativo de ordem individualista" – o direito de ser deixado sozinho e a não intrusão –, passando a "ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana" (DONEDA, 2006, p. 30).

Bruno Bioni afirma que "historicamente, a proteção de dados pessoais tem sido compreendida como o direito do indivíduo autodeterminar as suas informações pessoais", fazendo com que, "por meio do consentimento, o cidadão emita autorizações sobre o fluxo dos seus dados pessoais, controlando-os" (BIONI, 2018, p. 18). Tanto para Doneda quanto para Bioni, a proteção de dados pessoais relaciona-se com a capacidade do cidadão de *controlar suas informações*, em um contexto de expansão das técnicas de uso de informações pessoais, metadados, e fracasso dos modelos de *notice-and-consent*.[6] Essa concepção de *autodeterminacação informacional*, muito conectada com o pensamento europeu sobre dignidade e privacidade (WHITMAN, 2004), possui raízes históricas que precisam ser claramente compreendidas. É justamente esse paradigma que está sendo repensado por uma nova geração de pesquisadores europeus.

---

5 Por "matriz westiniana" refiro-me aos trabalhos de Alas Westin, que foram estruturantes no campo da proteção de dados pessoais no século XX.

6 A discussão mais sofisticada sobre o fracasso do modelo de *notice-and-consent*, que presume a ampla cognição dos termos de uso e políticas de privacidade online para livre contratação entre as partes, está no trabalho da filósofa Helen Nissembaum. Bioni apoia-se em Nissembaum para defender a abordagem de "integridade contextual", que exige normas substantivas que considerem contextos específicos para determinação das expectativas legítimas de privacidade e distorções que podem ser geradas por motivos comerciais (NISSEMBAUM, 2011).

1.1. A FORMAÇÃO DO MODELO TEÓRICO DOMINANTE

Conforme explicado pelo professor James Whitman, da Universidade de Yale, o debate estadunidense sobre privacidade e proteção de dados está muito conectado com concepções democráticas de controle da atividade governamental e de um necessário balanço entre segurança nacional e os direitos dos cidadãos de exercerem controle sobre as informações que são coletadas e tratadas pelo governo, e pelas empresas privadas (WHITMAN, 2004). É notável, nos trabalhos de Alan Westin (1929-2013) no final da década de 1960, um esforço para combater bases de dados opacas e ilegítimas, com recomendações principiológicas ao governo estadunidense sobre como garantir o consentimento dos titulares e a especificação de propósito, evitando bases de dados genéricas, como as sobre "militantes subversivos" e comunistas em um contexto pós-macartista. Em *Privacy and Freedom*, Westin teorizou a privacidade como a "capacidade de controlar o que é coletado sobre você" (WESTIN, 1967). Nas palavras de Marc Rotenberg, esse conceito tornou-se a "pedra basilar do direito moderno à privacidade", influenciando legislações estadunidenses e europeias durante as décadas de 1970 e 1980 (FOX, 2013).

De fato, os trabalhos de Westin influenciaram a formação dos "Fair Information Practice Principles" (FIPP) do Privacy Act de 1974 (TEUFEL, 2008), cujos princípios são (i) transparência, (ii) participação individual e consentimento, (iii) especificação de propósito, (iv) minimização de dados, (v) limitação temporal de uso, (vi) qualidade, integridade e segurança, (vii) *accountability* e (viii) auditagem. Essa mesma abordagem foi adotada pelo *U.S. Department of Health, Education and Welfare* (HEW)[7] e, posteriormente, pela Organização para Cooperação e Desenvolvimento Econômico no *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* de 1980, que reafirmou tais princípios regulatórios (HONDIUS, 1980).[8]

---

7 No relatório de 1973, intitulado *Records, Computers and the Rights of Citizens*, o capítulo "Redefinição do conceito de privacidade pessoal" discute expressamente conceitos de Alan Westin ("*privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extern information about them is communicated to others*") e Charles Fried ("*privacy is not simply an absence of information about us in the mind of others; rather, it is the control we have over information about ourselves*"), defendendo que registros que contenham informações pessoais sejam governados por procedimentos que permitam a *participação* do sujeito na delimitação do que será registrado e nos usos que serão feitos dessa informação. Ver o relatório completo em: https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Sou grato a Danilo Doneda por essa observação.

8 Na síntese de Doneda (2011, p. 100-101), os princípios defendidos pela OCDE em 1980 eram o da *publicidade* (autorização prévia para funcionamento de banco de dados, notificação de autoridade e produção de relatórios), da *exatidão* (tratamento com cuidado e correção, com dados fieis a realidade), da *finalidade* (utilização conforme finalidade comunicada ao interessado), do *livre acesso* (livre obtenção de cópias e controle dos dados) e *segurança física e lógica* (proteção contra extravio, destruição ou acesso não autorizado).

No final da década de 1980, uma importante distinção entre privacidade e proteção de dados pessoais foi feita pela Corte Constitucional alemã. O direito alemão, como notou um acadêmico na época, “mostra que a regulação da informação pessoal em computadores não pode depender da ideia jurídica de privacidade” (SCHWARTZ, 1989, p. 675). Ao invés de uma abordagem concentrada no “segredo”, o direito alemão prestou “atenção aos possíveis efeitos do processamento de informações para a autonomia humana” (SCHWARTZ, 1989, p. 676). Com os debates constitucionais em torno de um polêmico censo de 1983 – boicotado e acusado de intrusivo pela sociedade – a Corte alemã determinou que “o direito à autodeterminação informativa protege o indivíduo de coletas irrestritas, armazenamento, aplicação e transmissão dos dados pessoais” (SCHWARTZ, 1989, p. 689).[9]

Em 1995, a União Europeia realizou um grande esforço de harmonização de diferentes legislações sobre proteção de dados pessoais e aprovou a Diretiva de Proteção de Dados Pessoais, uma norma de padronização dos direitos fundamentais dos cidadãos europeus e de coordenação das competências regulatórias das Autoridades de Proteção de Dados Pessoais (BENNETT e RAAB, 1997). Em 2000, sob a influência de juristas europeus ligados a autoridades garantes de proteção de dados pessoais,[10] a Carta de Direitos Fundamentais da União Europeia[11] afirmou que “todas as pessoas têm direito à proteção de dados de caráter pessoal que lhe digam respeito” (art. 8º, I) e que os “dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei” (art. 8º, II).[12]

Essa perspectiva, dominante nos documentos da OCDE e no desenvolvimento do direito comunitário europeu, também é influente no Brasil, a partir de uma leitura sistemática do Código de Defesa do Consumidor (Lei 8.078/90) e do Marco Civil da Internet (Lei 12.965/14), que declara a proteção de dados pessoais como fundamento para uso da internet no país. Como sintetiza Laura Schertel Mendes, “o direito básico do consumidor à proteção de dados pessoais envolve uma dupla dimensão: (i) a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade

---

9 Para um estudo comparativo clássico, no âmbito da proteção de dados pessoais, entre o direito estadunidense, o alemão, o francês, o sueco e o canadense, ver Flaherty (1989).

10 Uma figura monumental, e de enorme influência no campo jurídico europeu, foi Stefano Rodotà (1933-2017). Para um apanhado geral de sua obra e seu papel central na formação dos “direitos digitais”, ver Doneda & Zanatta (2017).

11 Ver a Carta de Direitos Fundamentais em: http://www.europarl.europa.eu/charter/pdf/text_pt.pdf

12 No ensaio “A proteção de dados pessoais como um direito fundamental”, Doneda utiliza a ideia de “quatro gerações” das leis de dados pessoais na Europa desenvolvida por Viktor Mayer-Scönberger (DONEDA, 2011). Optei por não utilizar essa abordagem geracional para construir um modelo tipológico contrastável com a regulação do risco.

em face da coleta, processamento, utilização e circulação dos dados pessoais e (ii) a atribuição ao consumidor da garantia de controlar o fluxo de seus dados na sociedade" (MENDES, 2016, p. 7).[13]

De forma sintética e tipológica em sentido weberiano,[14] a formação de modelo teórico dominante se caracteriza pelos seguintes elementos: (i) a positivação de direitos individuais relacionados ao controle dos processos de coleta e tratamento de dados pessoais, (ii) a crença na conexão entre aumento do "poder de controle" e autonomia política em sociedades democráticas, a (iii) contratualização do consentimento, garantindo-se os direitos de informação clara, finalidade específica, prevenção de riscos e segurança das informações, e (iv) o reconhecimento da vulnerabilidade dos cidadãos, com a possibilidade de autoridades independentes para aplicação desses direitos.[15]

É esse modelo teórico que está sendo friccionado por uma nova abordagem da proteção de dados pessoais centrada na regulação do risco.[16] Trata-se menos de um processo de ruptura normativa na proteção de dados pessoais e mais como um processo de intensificação da regulação *ex ante* a partir de um ferramental teórico incorporado de outros campos. Detalha-se, a seguir, que abordagem teórica é essa e quais processos de reflexão ela provoca no debate contemporâneo sobre proteção de dados pessoais.

---

13 Além da preocupação com os "princípios de justiça", notável na obra dos acadêmicos dos EUA como Alan Westin, a teoria europeia de proteção de dados pessoais faz uma profunda conexão desses direitos com os direitos da personalidade. É notável a influência de Pierre Catala, professor francês que capitaneou os estudos de *informatique juridique* nos anos 1960, na obra de Danilo Doneda (2006), por exemplo. Doneda assume integralmente a tese de que quando o objeto dos dados é um sujeito de direito, a informação é *um atributo da personalidade*. Bioni, apoiando-se em Doneda e no civilista Gustavo Tepedino, defende que "os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas (…) também influenciam nessa perspectiva relacional da pessoa para com a sociedade (intersubjetividade)" (BIONI, 2018, p. 92).

14 Utilizo o recurso tipológico de Max Weber como *instrumento heurístico*, isto é, como um artefato intelectual para fins de discussão científica. Não se trata de um modelo necessariamente aderente com realidades sociais e jurídicas. Por ser um *tipo* ou um *modelo teórico*, ele é uma simplificação da realidade a partir da saturação de elementos históricos.

15 Como se trata de modelo tipológico, falo em *possibilidade* pois, no mundo real, esse é um tema de intensas disputas. EUA e Brasil, por exemplo, ainda não criaram autoridades independentes, apesar de fortes pressões de grupos políticos e sociedade civil.

16 Utilizo a expressão "friccionado" pois não creio que os modelos teóricos sejam diametralmente opostos ou que haja uma "substituição de paradigmas" no sentido dado por Thomas Kuhn. O friccionamento provoca essencialmente uma atividade reflexiva crítica. Agradeço a Diego Canabarro por me cobrar o esclarecimento desse ponto.

1.2. A EMERGÊNCIA DA REGULAÇÃO DO RISCO

O modelo teórico da regulação do risco, aplicável à proteção de dados pessoais, está relacionado a autores que analisam a "reformatação" da proteção de dados pessoais por um prisma mais complexo do direito regulatório, envolvendo mecanismos de contenção de abusividade e técnicas de prevenção e mitigação a riscos a direitos e liberdades em uma perspectiva coletiva. Nesse campo, encontram-se juristas contemporâneos majoritariamente localizados na Bélgica, Holanda e Inglaterra, como Serge Gutwirth & Yves Poullet (2013), Raphael Gellert (2015), Claudia Quelle (2015) e Alessandro Spina (2017).

A "regulação do risco", que foi inicialmente construída para lidar com problemas de ameaças à saúde com relação a novos medicamentos, alimentos industrializados e poluição ambiental (HUBER, 1983), coloca o *risco* como elemento central – a incerteza quantificável, nos termos de Frank Knight, ou a probabilidade de que um malefício vá ocorrer – e se concentra em processos de (i) reunião de informação e cognição de riscos, (ii) criação de regras e padrões de conduta e (iii) *enforcement* e monitoramento da modificação do comportamento social (HOOD, HOTHSTEIN e BALDWIN, 2001). Em termos gerais, esse modelo de "direito do risco" busca o isolamento de questões complexas e incertezas científicas para agentes decisórios de orientação marcadamente tecnicista – agências especializadas em cognição e controle de risco pela via do direito administrativo regulatório (MORGADO, 2017) –, que podem ou não seguir um modelo decisório baseado em precaução (SUNSTEIN, 2005),[17] e cria um conjunto de obrigações e normas jurídicas aplicáveis ao setor privado, com a intencionalidade de modificar o comportamento potencialmente danoso a níveis ótimos, evitar catástrofes e processos irreversíveis (POSNER, 2004), e aumentar o nível de informação disponível para qualificação dos processos de percepção dos riscos, inevitavelmente marcados por vieses culturais e visões de mundo contrastantes (SLOVIC, 2000).

Apesar de amplamente disseminado nos círculos internacionais (OCDE, 2008), é importante ressaltar que o desenvolvimento de teorias sobre regulação do risco surgiu em sociedades com regimes jurídicos com "formantes" enraizados na *common*

17 Por questões de economia textual, não há condições de um aprofundamento na rica discussão sobre as origens e polêmicas em torno do "princípio da precaução". Para uma profunda crítica ao princípio da precaução em sua forma mais radical e "paralisante", ver Sunstein (2005). Para uma análise do desenvolvimento do princípio da precaução no ambientalismo alemão, sua incorporação nos círculos intelectuais europeus e seu desenvolvimento frustrado em razão de casos levados à Organização Mundial de Comércio, ver Majone (2002). Para uma discussão sobre o princípio da precaução no campo da proteção de dados pessoais, ver os trabalhos de Costa (2012) e Gellert (2015). Para uma crítica à aplicação do princípio da precaução no campo da tecnologia enquanto bloqueio à inovação, ver Thierrer (2014).

law (SACCO, 1991) e forte tradição de *regulation* e capacidade normativa de agências reguladoras (SUNSTEIN, 1993). Essa tradição de "estudos sobre regulação" é recente em países como Brasil (FARIA, 2002), que passou por uma "adaptação tardia" do modelo de Estado regulador (LEVI-FAUR, 2005).

Raphaël Gellert, que realizou doutorado sob orientação de Serge Gutwirth na *Vrije Universiteit Brussel*, foi um dos primeiros autores a trazer a moldura teórica da "regulação do risco" – em especial a escola inglesa de regulação[18] – explicitamente para o campo da proteção de dados pessoais. Para Gellert, o modelo europeu gestado na década de 1990 têm se mostrado insuficiente para um cenário de constantes mudanças tecnológicas, expansão de dispositivos equipados com sensores, coleta massiva de dados biométricos e aumento das técnicas de "perfilização" (*profiling*) e predição de comportamentos. Em seu artigo, Gellert busca a substituição da matriz teórica de "informational privacy" de Alan Westin para uma matriz de "risk regulation" (GELLERT, 2015). Ao analisar o desenvolvimento da regulação do risco e seu caráter preventivo, focado na mitigação de danos coletivos, Gellert alega que as mudanças jurídicas europeias apontam uma clara ligação entre proteção de dados e regulação do risco.[19]

Gellert elenca evidências para esse argumento: primeiro, a recomendação de 2010 do Conselho da Europa de que a perfilização pode levar a "riscos significantes para as liberdades e direitos individuais"; segundo, o relatório sobre aplicação dos princípios da Convenção 108 sobre coleta e processamento de dados biométricos, que advoga pelo "uso do princípio da precaução, um princípio explícito de regulação do risco" (GELLERT, 2015, p. 7). Gellert afirma também que o teste de proporcionalidade sobre "finalidade legítima" – que exige uma análise contextual do modo como os dados são analisados e o consentimento informado dado pelo sujeito que teve o dado

---

18 Por "escola inglesa de regulação" quero designar o conjunto de estudos e teorias desenvolvidas na London School of Economics, no Centre for Analysis of Risk and Regulation (CARR). Os autores mais influentes dessa escola são Martin Lodge, Robert Baldwin, Martin Cave, Christopher Hood e Julia Black. Anteriormente a fundação da CARR, os principais estudos ingleses sobre teoria do risco foram financiados pelo Economic and Social Research Council (ESRC). Sobre o centro, ver http://www.lse.ac.uk/accounting/CARR/aboutUs/Home.aspx

19 Tanto Gellert (2015) quanto Quelle (2015) atentam para a distinção entre *risk regulation* e *risk-based regulation.* A "regulação baseada em risco" é distinta e problemática, pois assume que tudo é passível de gestão de risco e que a intensidade da regulação pode ser desenhada a partir de variações e intensidades de riscos. Nos estudos ingleses sobre regulação, são muitas as críticas sobre a quantificação da análise de risco (*quantitative risk assessment*), a opacidade da interpretação dos dados coletados pelo regulador, a falsa objetividade dessa quantificação, a dificuldade de avaliar danos potenciais, a indefinição sobre o que são "riscos aceitáveis" e o problema de considerar *frequências* ao invés de *consequências* (HUTTLER, 2005, p. 5-10).

coletado – é uma forma de realizar uma "*análise de risco* aos riscos a direitos fundamentais" (GELLERT, 2015, p. 9).

A existência de autoridades com alta expertise técnica, como os *Data Protection Authorities* (DPA) e o grupo de trabalho *Article 29 Data Protection Working Party,* seria outra evidência de uma racionalidade regulatória de risco, fundada no conhecimento técnico e na criação de obrigações de produção de informação sobre riscos ao setor privado (SUNSTEIN, 2002), como os "estudos de impacto à privacidade" (GELLERT, 2015, p. 11-12).[20] Alessandro Spina, em ensaio recente para o *European Journal of Risk Regulation*, defende uma agenda de pesquisas capaz de unir "regulação do risco e governança dos dados". Em argumento semelhante ao de Gellert (2015), Spina alega que, ao menos na União Europeia, está se testemunhando uma espécie de "risquificação" do direito de proteção de dados pessoais.

A ideia de risquificação também é assumida por Claudia Quelle, doutoranda na Universidade de Tilburg. Em um ensaio sobre o potencial conflito entre uma abordagem baseada em risco e a teoria dos direitos fundamentais, Quelle argumenta "a proteção de dados pode ser caracterizada como regulação do risco" (QUELLE, 2015). Para Quelle, o direito da proteção de dados "foi desenvolvido para regular o possível dano de tecnologias da informação bem como proteger os direitos fundamentais dos indivíduos" e "acima disso, a proteção de dados pessoais também é baseada no risco: o conceito de risco, em termos de severidade e probabilidade, é utilizado para calibrar obrigações jurídicas" (QUELLE, 2015, p. 1).

No modelo tipológico da regulação do risco, a proteção de dados pessoais "risquificada" passa a ter os seguintes elementos: (i) instrumentos de tutela coletiva e participação de entidades civis no diálogo preventivo com autoridades independentes de proteção de dados pessoais, (ii) obrigações e instrumentos de regulação *ex ante* atribuídas aos controladores para identificação de riscos a direitos e liberdades fundamentais, (iii) disseminação de metodologias de "gestão de risco" e calibragem entre *riscos* gerados pelo tratamento e uso de dados pessoais e *imunidades jurídicas* construídas pela discussão ética sobre os limites do progresso técnico.

---

20 Como será discutido posteriormente, na Europa avançam instrumentos regulatórios de "análise de impacto de proteção de dados pessoais" (*Personal Data Impact Assessment*), em uma aproximação aos Estudos de Impacto Ambiental (EIA) desenvolvidos no campo ambiental (WRIGHT e DE HERT, 2012).

2. O SIGNIFICADO DA RISQUIFICAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS

Conforme discutido acima, por *risquificação da proteção de dados pessoais* entende-se esse processo de reformatação jurídica a partir da ampliação da tutela coletiva e sua imbricação com a autoridade independente de proteção de dados pessoais, a disseminação de instrumentos regulatórios *ex ante* e o uso intensivo de metodologias de gestão de risco e calibragem entre riscos, inovações e imunidades – um processo de "negociação coletiva" (TUBARO e CASILLI, 2018) que supera a tradicional concepção bilateral entre sujeito de direito e aquele que processa dados pessoais pessoais.

É consenso na literatura que a risquificação é um processo eminentemente europeu (GELLERT, 2015; QUELLE, 2015; SPINA, 2017). É a partir de uma leitura atenta da *General Data Protection Regulation* (GDPR) que se compreende a centralidade e complexidade da regulação do risco nos mercados digitais intensivos em dados pessoais.

2.1. EVIDÊNCIAS DA REGULAÇÃO DO RISCO NA LEGISLAÇÃO EUROPEIA

Na União Europeia, a aprovação do Regulamento n. 679/2016 (*General Data Protection Regulation*)[21] trouxe outra perspectiva regulatória para a proteção de dados pessoais a partir de uma série de instrumentos de regulação *ex ante* e controle de riscos. É notável que a palavra "risco" apareça 74 vezes no Regulamento. O Regulamento impõe que o responsável pelo tratamento de dados pessoais possui a responsabilidade de determinar se o tratamento "implica em risco para os direitos e liberdades das pessoas titulares". O Regulamento faz uma separação entre "risco" e "risco elevado" e dá exemplos de critérios objetivos para determinação do risco em determinado contexto. Por exemplo, uma empresa que pretenda desenvolver tecnologia de reconhecimento facial e coleta de dados biométricos a partir da análise de filmagens feitas por drones em áreas abertas claramente trará risco elevado de lesão a direitos fundamentais, tanto em razão da coleta de *dados biométricos* (considerados dados sensíveis que só podem ser coletados para finalidades específicos e com consentimento informado dos titulares), quanto em razão da coleta ser feita a partir de *áreas geográficas abertas*.

---

21 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

Como forma de mitigação de tais riscos, o regulador europeu afirma expressamente que a "identificação dos riscos relacionados com o tratamento", sua "avaliação em termos de origem, natureza, probabilidade e gravidade", bem como a "identificação das melhores práticas para atenuação dos riscos"[22] poderão ser obtidas por (i) códigos de conduta aprovados, (ii) certificações aprovadas, e (iii) orientações fornecidas pelo encarregado pela proteção de dados pessoais. Nota-se, aqui, uma clara abordagem de "co-regulação" (HIRSCH, 2013), fortalecendo o papel dos próprios entes regulados na definição de códigos de melhores práticas, certificações e orientações profissionais.[23] A legislação europeia também adota uma política de incentivo de *privacy by design*, ou seja, que preocupações com privacidade e violações de direitos sejam consideradas na concepção de softwares e hardwares que dependem da coleta de dados (LIMA e BIONI, 2015).

Além de riscos de perfilização, discriminação e limitação de direitos e liberdades, o Regulamento Europeu fala em "riscos para a segurança dos dados", relacionados a *data breaches*, ataques hackers e acesso não autorizado a dados pessoais transmitidos. A norma europeia impõe que "o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a anonimização e cifragem [criptografia]" (art. 32). Uma das formas de mensurar tais riscos – de discriminação ou de segurança da informação – é a realização de uma "avaliação do impacto à proteção de dados"[24].

As metodologias de avaliação de impacto à proteção de dados não são explicitadas no Regulamento de 2016, o que tem fomentado enormes discussões sobre o papel a ser desempenhado pela *Article 29 Working Party* e pelos servidores e

---

22 Para Spina, a geração de riscos a direitos e liberdades é reforçada pelo fato de que produtos industriais, cujos riscos eram controlados por arranjos regulatórios tradicionais (*e.g.* segurança do consumidor), agora estão se tornando "inteligentes". "Sensores, micro-dispositivos geradores de dados, objetos vestíveis conectados e a Internet das Coisas transformam nossa experiência do mundo e apresentam outra camada de riscos para os consumidores", diz Spina (2017, p. 89). Para ele, a complexidade de riscos criada pela inovação digital demanda a criação de novos "sistemas de controle regulatório" que não se limitem ao cumprimento formal de regras e normas de interesse público, mas que foquem nos aspectos técnicos da coleta de informações e nos aspectos éticos do real impacto dessas regras (SPINA, 2017, pp. 90-92).

23 Em artigo que dialoga com Dennis Hirsch e Colin Bennet, discuti alguns dos impasses para corregulação no Brasil e as pressões do setor privado, entre 2010 e 2012, para manutenção de um modelo de autorregulação, com interferência mínima de uma autoridade independente (ZANATTA, 2015).

24 De acordo com Wright (2012), o desenvolvimento de *impact assessments* é fruto de pressões de consultorias internacionais, empresas de tecnologia e *policy experts* do setor privado na Europa. Trata-se de uma forma de *internalização* do processo de balanceamento entre inovação e riscos a direitos para dentro das empresas, abrindo mais espaço para experimentação e autorregulação, ao invés de uma perspectiva de comando-e-controle rígida, proibitiva e punitiva.

profissionais de autoridades independentes de proteção de dados pessoais (QUELLE, 2015). Até o momento não há pesquisas de fôlego sobre as distinções, diferenças ou convergências entre esse tipo específico de avaliação de impacto e instrumentos regulatórios mais disseminados como as diferentes modalidades de avaliação de impacto ambiental.[25] A hipótese avançada por Claudia Quelle (2015) é que as metodologias serão influenciadas pela teoria do *balanceamento de direitos fundamentais* desenvolvido pela Corte Europeia de Justiça, onde as violações de direitos são analisadas em casos concretos. O problema, no entanto, é que a violação de direito é *potencial* e não *real*. É de se esperar, portanto, um crescente tecnicismo por parte da *Article 29 Working Party* para criação de metodologias de identificação de *riscos potenciais* e novas taxonomias para compreensão do que há de mais avançado nas técnicas da ciência computacional para análise de dados, bem como a crescente imbricação entre vazamento de dados pessoais (incidentes de segurança) e ameaças a direitos, o que tende a aumentar a importância política da matemática aplicada à criptografia e técnicas de "descentralização da privacidade" por *blockchain* (ZYSKIND, 2015).

Do mesmo modo que desastres ambientais prováveis precisam ser informados aos titulares de direitos e às comunidades, a nova lei de dados pessoais obriga que o responsável pelo tratamento deverá informar imediatamente o titular dos dados que foram violados "quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias". Importante ressaltar que o GDPR cria instrumentos de tutela coletiva para que organizações não governamentais possam responsabilizar empresas e governos por negligência ou por danos coletivos à privacidade e proteção de dados pessoais. Não é sem razão que Max Schrems, ativista austríaco que criou um caso paradigmático contra a coleta de dados pessoais pelo Facebook, criou a ONG *None Of Your Business (NOYB)* e arrecadou 250 mil de euros em plataformas de *crowdfunding* para ajuizamento de ações coletivas com base no GDPR.[26] Uma das principais características da risquificação é justamente a habilitação para que entidades civis tenham legitimidade ativa em processos judiciais contra empresas que tenham violado as normas de proteção de dados pessoais, com a criação de tipos específicos de *data protection class action* ou *privacy class action* (SROUJI e DOLHEM, 2017). Essa "coletivização da tutela" é coerente com a falha, apontada por

25 Esse é um tópico que tem sido avançado no Instituto de Energia e Ambiente da USP, em colaboração com os professores Ricardo Abramovay e Evandro Moretto. Sobre a pluralidade de métodos de avaliação de impactos ambientais, ver Sánchez (2013).

26 Scherms também é reconhecido na literatura especializada. Ele é conhecido por criar as mais populares *privacy class action* na Europa (SROUJI e DOLHEM, 2017).

Helen Nissembaum (2011), do ideário liberal clássico de que as pessoas possuem livre compreensão dos contratos, são capazes de consentir livremente com os termos de uso de aplicações de internet e podem defender seus direitos em juízo.[27]

Apesar da zona cinzenta sobre como ocorrerão, em detalhes, as avaliações de impacto à proteção de dados pessoais, os relatórios que devem ser enviados às autoridades independentes e os mecanismos de certificação, é fato que os instrumentos de regulação *ex ante* já estão previstos no GDPR. Do mesmo modo, mesmo que não haja ações coletivas notáveis sobre proteção de dados pessoais, há instrumentos processuais previstos no regulamento, o que tem fomentado o surgimento de ONGs especializadas para ajuizamento de ações coletivas e formulação de litígios estratégicos em proteção de dados pessoais. A necessidade de avaliação ética e potencialmente danosa das empresas de tecnologia – especificamente as intensivas em dados – também tem aquecido um mercado interdisciplinar de *compliance* e comitês de autorregulação e identificação de melhores práticas. Tudo isso faz parte do fenômeno de risquificação de que falam os europeus e que poderá ser progressivamente visto no Brasil.

2.2. EVIDÊNCIAS DA REGULAÇÃO DO RISCO NA LEGISLAÇÃO BRASILEIRA

A adoção de instrumentos regulatórios de risco não é fenômeno exclusivo da Europa no âmbito da proteção de dados pessoais. No Brasil, o Projeto de Lei 5.276/16, apresentado por Dilma Rousseff após elaboração participativa conduzida pelo Ministério da Justiça, prevê a elaboração de "estudos de impacto à privacidade" quando o responsável pelo tratamento de dados utilizar a hipótese de legítimo interesse para dispensa do consentimento informado (art. 10). Prevê, também, que "o responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares" (art. 47). O incidente deve conter informações sobre natureza dos dados pessoais afetados, informações sobre os titulares envolvidos, a indicação das medidas de segurança e encriptação, os riscos relacionados ao incidente, e as medidas que serão adotadas para reverter ou mitigar os efeitos de prejuízo.[28]

27 Essa crítica ao ideário liberal clássico é um dos pontos centrais da teoria consumerista brasileira, que reconhece a hipervulnerabilidade dos consumidores e garante às organizações civis a legitimidade para ações civis públicas.

28 É notável que, na ausência de uma autoridade de proteção de dados pessoais e de aprovação do PL 5276/16, o Ministério Público do Distrito Federal e Territórios (MPDFT) tenha criado sua própria Comissão de Proteção de Dados Pessoais em novembro de 2017, com poderes para instruir inquéritos civis em casos de incidentes de segurança a ajuizamento de ações civis públicas para defesa de direitos coletivos relacionados à proteção de dados pessoais.

Infelizmente, o Projeto de Lei 5.276/16 não possui normas muito desenvolvidas sobre as avaliações de impacto à proteção de dados pessoais e outras obrigações que deveriam ser assumidas de modo *ex ante* pelos controladores e processadores de dados pessoais. Talvez isso se explique pelo fato de que as discussões estruturantes tanto do projeto de lei elaborado pelo governo de Dilma como do Projeto de Lei do Senado 330/2013 ocorreram *antes da guinada ao risco* do *General Data Protection Regulation* (GDPR). Desse modo, o direito brasileiro aproxima-se mais do modelo teórico dominante da autodeterminação informacional e menos do modelo teórico da regulação do risco, apesar das evidências e pontos de convergência já apontados.

Por fim, importante ressaltar, como lembra Laura Mendes (2016), que o Marco Civil da Internet e o Código de Defesa do Consumidor impõem a tutela da personalidade do consumidor contra os riscos. É direito básico do consumidor "a proteção da vida contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos" (art. 6º, I, Lei 8.078/90). Há também o direito básico às informações sobre riscos que produtos e serviços apresentam (art. 6º, II, Lei 8.078/90). É certo que tradicionalmente, na linha da seção que trata de "proteção à saúde e segurança" no CDC, o risco tem sido compreendido como risco à segurança física (*safety*). Porém, isso não impede um trabalho dogmático de ressignificação do conceito de risco de modo a aproximá-lo da concepção de segurança informacional (*security*). Isso traria impactos ao próprio modelo de responsabilidade civil objetiva, independente da existência de culpa, em casos de "informações insuficientes ou inadequadas" (art. 14, Lei 8.078/90). Tal interpretação seria aderente com a recepção da teoria do risco no Código Civil,[29] que deixa claro no parágrafo único do artigo 927 que "haverá obrigação de reparar o dano, independentemente de culpa (...), quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem". Mais uma vez, a questão gira em torno da interpretação casuística sobre *o que é gerar risco para os direitos de outrem.*

De todo modo, nota-se no direito brasileiro vigente um enfoque eminentemente civil, em termos de responsabilidade civil e instrumentos de controle *ex post*, fazendo com o que risco sirva de gatilho para obrigações de reparar danos. Como visto, a risquificação provoca uma mudança de rota para a prevenção de danos *antes que eles ocorram* e instrumentos regulatórios que incrementem o nível de informação e cognição de riscos por autoridades especializadas, bem como um conjunto de

29 Não é objetivo desse artigo discutir as origens da "teoria do risco" e sua aplicabilidade no direito civil, ambiental e trabalhista. Sobre o tema, ver os conhecidos estudos de Benjamin (1993) e Pereira (1994).

obrigações às empresas de tecnologia, impostas pelo poder público, condicionando a atividade empresarial a comportamentos potencialmente éticos, no sentido de constante reavaliação de potenciais ameaças a direitos, “chilling effects” em razão de aparatos de vigilância (WRIGHT e RAAB, 2012) e exposição de informações sensíveis que poderiam retroalimentar práticas discriminatórias estruturadas por algoritmos (PASQUALE, 2015). O direito brasileiro ainda está longe disso.

CONCLUSÃO

A compreensão do processo de risquificação é relevante por, pelo menos, três motivos. Primeiro, pois significa a superação de um olhar voltado exclusivamente à regulação *ex post*, ou seja, às formas de punição e reparação por instrumentos civis e penais após a ocorrência de um dano, retomando um debate sobre precaução e proteção de dados pessoais (COSTA, 2012). Segundo, pois a risquificação da proteção de dados pessoais força uma aproximação com teorias de “regulação do risco” utilizadas em outras áreas como nanotecnologia, engenharia genética e regulação ambiental (ADAMS, 2009) – e muito pouco conhecidas no debate sobre proteção de dados pessoais, notadamente marcado por um viés de direito civil e direito do consumidor. Terceiro, pois a risquificação incita a formulação de novos problemas pouco discutidos na literatura brasileira: quais os riscos sociais existentes em inovações tecnológicas e processos de coleta e análise de dados pessoais? Como empresas de tecnologia e governos, que fazem uso intensivo de dados, podem dimensionar e mitigar “riscos a liberdades fundamentais” (SPINA, 2017)? Como contestar, individualmente e coletivamente, “análises de impacto à proteção de dados pessoais” (WRIGHT e DE HERT, 2012) eivadas de vício ou mal formuladas? Como combinar o direito civil com um conjunto regulatório, que combina técnicas de regulação de comando-e-controle e instrumentos de corregulação, para formação de um “direito do risco” (BARONE, 2006)?

Essas são apenas algumas questões, não respondidas, que compõem parte da agenda de risquificação da proteção de dados pessoais e que, por influência do debate europeu, aos poucos se descortina na América Latina e no Brasil. Além dessas questões, a agenda de pesquisa do campo pode se direcionar para uma profunda comparação entre o desenvolvimento histórico da tutela coletiva e da regulação do risco no campo ambiental e a atual risquificação da proteção de dados pessoais, em busca de divergências, convergências e aproximações entre os instrumentos de regulação *ex ante*.

Por fim, é preciso um debate qualificado, por toda a comunidade acadêmica e prática, sobre os "riscos da risquificação"[30] em proteção de dados pessoais. Ou seja, a possibilidade de que uma "abordagem baseada em riscos" no Brasil seja utilizada estrategicamente para deslocar a linguagem dos direitos fundamentais e isolar o cidadão comum dos impasses jurídicos da proteção de dados pessoais, fazendo com que as tensões e "negociações coletivas" ocorram somente entre empresas de tecnologia, autoridade reguladora e entidades civis altamente especializadas. Há também o risco de que, diante de metodologias mal formuladas para identificação de potenciais lesões a direitos por parte de empresas intensivas em dados, haja alto grau de judicialização de medidas regulatórias e administrativas, com o travamento estratégico do processo de regulação por interesses econômicos específicos. Pensar nessa nova moldura teórica implica, também, no enfrentamento dessas difíceis questões.

REFERÊNCIAS

AYRES, I., & BRAITHWAITE, J. *Responsive Regulation: transcending the deregulation debate.* Oxford: Oxford University Press, 1992.

ADAMS, J.. *Risco.* São Paulo: Senac, 2009.

ANGARITA REMOLINA, N. Latin American and Protection of Personal Data: facts and figures (1985-2014). *University of Los Andres Working Paper* , 1-14, 2014.

BALDWIN, R., & BLACK, J. Really Responsive Regulation. *LSW Law, Society and Economy Working Papers , 15*, 1-44, 2008.

BALDWIN, R., CAVE, M., & LODGE, M. Regulation: the field and the developing agenda. In R. Baldwin, M. Cave, & M. Lodge, *The Oxford Handbook of Regulation* (pp. 2-25). Oxford: Oxford University Press, 2010.

BALDWIN, R., LODGE, M., & CAVE, M. *Understanding Regulation.* Oxford: Oxford University Press, 2012.

BARONE, A. *Il Diritto Del Rischio.* Milano: Giuffrè, 2006.

BENJAMIN, A. H. *Dano ambiental: prevenção, reparação e repressão.* São Paulo: Editora Revista dos Tribunais, 1993.

BENNETT, C., & RAAB, C. The Adequacy of Privacy: the European Union Data Protection Directive and the North American Response. *The Information Society: an international journal* , 245-264, 1997.

BIONI, B. *Autodeterminação informacional: qual o papel e os limites do consentimento na proteção dos dados pessoais.* São Paulo: Grupo Gen, 2018 (no prelo).

COSTA, L. Privacy and the precautionary principle. *Computer Law & Security Review , 28* (1), 14-24, 2012.

30 Sou grato a Bruno Bioni e Danilo Doneda pela discussão sobre os riscos da risquificação.

DE HERT, P., & PAPAKONSTANTINOU, V. The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review , 28*, 130-142, 2012.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico , 12*, 91-108, 2011.

DONEDA, D. *Da Privacidade à Proteção de Dados Pessoais.* Rio de Janeiro: Renovar, 2006.

DONEDA, D., & ZANATTA, R. A. F. *Rodotà e o equilíbrio entre direito, tecnologia e política*, *Jota*: https://www.jota.info/opiniao-e-analise/artigos/rodota-e-equilibrio-entre-direito-tecnologia-e-politica-28062017. Acesso em 22 de janeiro de 2018.

FARIA, J. E. *Direito, Regulação e Democracia.* São Paulo: Fundação Perseu Abramo, 2002.

FEDERAL TRADE COMMISSION. *Internet of Things: privacy and security in a connected world.* Federal Trade Commission. Washington D.C.: FTC, 2015.

FLAHERTY, D. *Protecting Privacy in Surveillance Societies.* Chapel Hill: University of North Carolina Press, 1989.

FOX, M. *Alan F. Westin, who transformed privacy debate before the web era, dies at 83*, *New York Times*. Disponível em: http://www.nytimes.com/2013/02/23/us/alan-f-westin-scholar-who-defined-right-to-privacy-dies-at-83.html. Acesso em 22 de janeiro de 2018.

GUTWIRTH, S., & POULLET, Y. Introduction. In S. Gutwirth, Y. Poullet, R. Leenes, & P. de Hert, *European Data Protection: coming of age* (pp. 1-10). Dordrecht: Springer, 2013.

GELLERT, R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law , 5*, 3-20, 2015.

HUBER, P. The Old-New Division in Risk Regulation. *Virginia Law Review , 69* (6), 1025-1107, 1983.

HIRSCH, D. Going Dutch? Collaborative Dutch privacy regulation and the lessons it holds for the US. *Michigan State Law Review , 83*, 85-162, 2013.

HONDIUS, F. Data law in Europe. *Stanford Journal of International Law , 16*, 87-102, 1980.

HOOD, C., HOTHSTEIN, H., & BALDWIN, R. *Government of Risk.* Oxford: Oxford University Press, 2001.

HUTLER, B. The Attractions of Risk-Based Regulation: accounting for the emergence of risk ideas in regulation, *Center for Analysis of Risk and Regulation Working Paper*, Discussion paper n. 3, 2005.

KNIGHT, F. *Risk, Uncertainty and Profit.* New York: Cosimo, 2005.

LEVI-FAUR, D. The global diffusion of regulatory capitalism. *The Annals of the American Academy of Political and Social Science*, (pp. 12-32). New York, 2005.

LIMA, C. R., & BIONI, B. A proteção dos dados pessoais na fase da coleta. In N. De Lucca, A. Simão Filho, & C. Lima, *Direito & Internet III: Marco Civil da Internet.* São Paulo: Quartier Latin. 2015.

NISSEMBAUM, H. A contextual approach to privacy online. *Deadalus , 140* (4), 32-48, 2011.

MAJONE, G. The Precautionary Principle and Its Policy Implications. *Journal of Common Market Studies , 40*, 89-110, 2002.

MAJONE, G., & LA SPINA, A. *Lo Stato Regolatore.* Milano: Il Mulino, 2000.

MENDES, L. S. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor , 105*, 1-30, 2016.

MENDES, L. S. O direito fundamental à proteção de dados pessoais. *Revista de Direito do Consumidor , 79*, 45-81, 2011.

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

MORGADO, C. *O Direito Administrativo do Risco: a nova intervenção estatal sob o enfoque da segurança alimentar.* Rio de Janeiro: Editora Gramma, 2017.

OCDE. *Summary of Discussion on Risk and Regulation at the Meeting of the Group on Regulatory Policy.* Bruxelas: OECD, 2008.

OHLAUSEN, M. The Internet of Everything: data, networks and opportunities. *The Internet of Everything.* Washington: U.S. Chamber of Commerce, 2015.

QUELLE, C. Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level? *Tilburg Law School Research Paper* , 1-36, 2015.

PASQUALE, F. *The Black Box Society: the secret algorithms that control money and information.* Cambridge: Harvard University Press, 2015.

PEREIRA, C. M. *Responsabilidade civil* (5 ed.). Rio de Janeiro: Editora Forense, 1994.

POSNER, R. *Catastrophe: Risk and Response.* New York: Oxford University Press, 2004.

PROSSER, T. *The Regulatory Enterprise.* Oxford: Oxford University Press, 2010.

SUNSTEIN, C. *After the Rights Revolution: reconceiving the regulatory state.* Cambridge: Harvard University Press, 1993.

SUNSTEIN, C. *Laws of Fear: beyond the Precautionary Principle.* Cambridge: Cambridge University Press, 2005.

SUNSTEIN, C. *Risk and Reason.* Cambridge: Cambridge University Press, 2002.

SACCO, R. Legal formants: a dynamic approach to comparative law. *The American Journal of Comparative Law , 39* (1), 1-34, 1991.

SÁNCHEZ, L. E. *Avaliação de Impacto Ambiental: conceitos e métodos.* São Paulo: Oficina de Textos, 2013.

SANDIN, P. The Precautionary Principle and the Concept of Precaution. *Environmental Values , 13*, 461-475, 2004.

SCHWARTZ, P. The Computer in German and American Constitucional Law. *American Journal of Comparative Law , 37*, 675-705, 1989.

SCHWARTZ, P. Property, Privacy, and Personal Data. *Harvard Law Review , 117*, 2057-2128, 2004.

SCHNEIER, B. *Schneier on Security.* New York: Wiley, 2009.

SEVIGNANI, S. The commodification of privacy on the Internet. *Science and Public Policy , 40* (6), 733-739, 2013.

SLOVIC, P. *The Perception of Risk.* London: Earthscan, 2000.

SPINA, A. A Regulatory Mariage de Figaro: risk regulation, data protection, and data ethics. *European Journal of Risk Regulation , 8*, 88-94, 2017.

SROUJI, J., & DOLHEM, M. Class action and data privacy in the USA and Europe: effective deterrent or ill-founded approach to compliance. *Journal of Data Protection & Privacy , 1* (3), 294-305, 2017.

ROESER, S., HILLERBRAND, R., SANDIN, P., & PETERSON, M. *Essentials of Risk Theory.* Amsterdam: Springer, 2007.

RODOTÀ, S. *Elaboratori elettronici e controllo sociale.* Bologna: Il Mulino, 1973.

TUBARO, P., & CASILLI, A. Notre vie privée, un concept négociable. *Le Monde* , pp. 1-4, 2018.

TEUFEL, H. *Privacy Policy Guidance Memorandum: Fair Information Practice Principles.* Washington D.C.: U.S. Department of Homeland Security, 2008.

THIERER, A. Privacy Law's Precautionary Principle Problem. *Maine Law Review , 66*, 468-488, 2014.

WEBER, R. Internet of things–Need for a new legal environment? *Computer Law & Security Review , 25* (6), 522-527, 2009.

WESTIN, A. *Privacy and Freedom.* New York: Athenum, 1967.

WESTIN, A. Science, Privacy and Freedom: issues and proposals for the 1970s. *Columbia Law Review , 66* (6), 1003-1050, 1966.

WHITMAN, J. Two Western Cultures of Privacy: dignity versus liberty. *Yale Law Journal , 113*, 1153-1260, 2004.

WRIGHT, D., & DE HERT, P. *Privacy Impact Assessment.* Amsterdam: Springer Netherlands, 2012.

WRIGHT, D., & RAAB, C. Constructing a surveillance impact assessment. *Computer Law & Security Review , 28* (6), 613-626, 2012.

ZANATTA, R. A. F. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. In N. De Lucca, A. Simão Filho, & C. Lima, *Direito & Internet III: Marco Civil da Internet*. São Paulo: Quartier Latin, p. 447-470, 2015.

ZYSKIND, G. Decentralizing privacy: using blockchain to protect personal data. *Security and Privacy Workshops IEEE , 5*, 180-184, 2015.