MODELOS REGULATÓRIOS PARA PROTEÇÃO DE DADOS PESSOAIS

Guilherme Berti de Campos Guidi[1]

Introdução

A privacidade e a proteção de dados pessoais, a também chamada *data privacy*, são temas que têm ocupado espaços cada vez maiores, não mais apenas nos congressos acadêmicos e painéis de discussão, mas também na grande mídia[2]. O cidadão comum, alheio talvez aos grandes debates teóricos, se não tem ainda completa ciência da proteção que pode reclamar para seus dados pessoais, tem no mínimo maiores chances de ser exposto ao assunto.

Tal movimento nos dá importante sinal, pois se mesmo o cidadão comum passa a ter consciência desses seus direitos, ainda que os estudiosos continuem questionando cada vírgula do que foi escrito sobre o assunto, nenhuma dúvida resta sobre a existência de *alguma coisa, algum direito à privacidade e à proteção dos dados.* O presente trabalho não objetiva discutir a existência ou inexistência de um direito à tutela dos dados pessoais, nem seus eventuais contornos, mas sim discutir estratégias regulatórias colocadas em prática, tendo como premissa a existência de tal direito e seu conteúdo já solidificado, ao menos em princípio, na doutrina sobre o assunto[3]. Dado este enorme passo, devemos, entretanto, atentar a uma questão relevante e anterior a qualquer discussão sobre direitos e deveres específicos:

---

[1] Bacharel e Mestre em Direito Civil pela Faculdade de Direito da Universidade de São Paulo - USP, especializado em Direito Digital pela Escola de Direito de São Paulo da Fundação Getúlio Vargas. Pesquisador do Instituto de Tecnologia e Sociedade do Rio de Janeiro, pesquisador colaborador do Grupo de Ensino e Pesquisa em Inovação da Fundação Getúlio Vargas (GEPI/FGV-SP). Membro da Comissão Permanente de Estudos sobre Tecnologia da Informação do Instituto dos Advogados de São Paulo, membro do Comitê de Compliance Digital da *Legal, Ethics and Compliance*. Sócio do escritório Francisco Rezek Sociedade de Advogados.

[2] A tal respeito, confira-se, por exemplo: RONCOLATO, Murilo. Por que debater a Lei de Proteção de Dados Pessoais?. **O Estado de São Paulo Online**, 28 jan. 2015. Disponível em: <http://link.estadao.com.br/noticias/geral,por-que-debater-a-lei-de-protecao-de-dados-pessoais,10000029762>. Acesso em 19.01.17. PEDUZZI, Pedro. MJ finaliza nova versão de anteprojeto sobre proteção de dados na internet. **Agência Brasil EBC**, 19 out. 2015. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2015-10/mj-finaliza-nova-versao-de-anteprojeto-sobre-protecao-de-dados-na-internet>. Acesso em 19.01.17. ANGWIN, Julia. Protecting Your Digital Privacy Is Not as Hard as You Might Think. **Consumer Reports**, 20 set. 2016. Disponível em: <http://www.consumerreports.org/privacy/protecting-your-digital-privacy-is-not-as-hard-as-you-might-think/>. Acesso em 19.01.17.

[3] Sobre os fundamentos da proteção dos dados pessoais, confira-se: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006; e LEONARDI, Marcel. **Tutela e privacidade na Internet**, São Paulo: Saraiva, 2012.

como regular?

O Brasil, chegando atrasado no debate, tenta compensar o tempo perdido, estando o Congresso Nacional pressionado para aprovar algum dos projetos de lei sobre o assunto hoje em trâmite. O que o Congresso discute, no entanto, são propostas que adotam estratégias muito diferentes para abordar a questão[4], pautando o debate nos direitos e deveres que cada projeto promete, sem perceber que a proteção de dados pessoais deve ser pensada antes como política pública, e não como simples objeto passivo para a regulação. Para isso, é necessário definir, antes de mais nada, qual será a abordagem regulatória adotada, de modo que a tutela da privacidade esteja inserida em um sistema coeso de normas.

Os projetos de lei em discussão no Congresso Nacional, em sua maior parte, adotam modelos legais consolidados, sendo o modelo vigente na União Europeia - ou melhor, o modelo vigente até maio de 2018, dadas as recentes reformas[5] - o mais influente nas propostas. Mas mesmo que nossas leis copiassem o que há de melhor lá fora, nem sempre tais modelos são suficientes para garantir direitos enquanto também se incentiva o desenvolvimento tecnológico e econômico, sobretudo nos negócios digitais. A maioria dos modelos atuais tem grande foco em legislação garantista, protetiva, que impõe igualmente diversos deveres aos interessados nos dados alheios. Outros, por sua vez, relegam à autorregulação, ao direito contratual e ao Judiciário a tutela de direitos.

Tal discussão, geralmente, traz um viés essencialmente protetivo ao usuário, sem considerar, por outro lado, os interesses econômicos e o interesse geral no desenvolvimento tecnológico e na inovação. Por essa razão, é necessário justamente dar um passo atrás e pensar em como se pretende fazer com que os titulares tenham seus direitos respeitados, que as empresas cumpram suas obrigações e que a sociedade como um todo considere a privacidade um direito essencial, como efetivamente é.

Para que possamos sequer iniciar tal debate, devemos primeiro verificar, mapear, o que existe, suas características principais, de modo a revelar a estratégia central de cada modelo para regular a coleta e o uso dos dados pessoais, e é esse o objetivo deste artigo.

Analisaremos, para tanto, brevemente os pontos principais de três modelos distintos: o modelo europeu, o modelo norte-americano e o modelo uruguaio. A escolha desses países

[4] Entre os projetos mais relevantes, temos o Projeto de Lei nº 4.060/2012 e Projeto de Lei nº 5.276/2016, da Câmara dos Deputados, e os Projetos nº 181/2014, 131/2014 e 330/2013, do Senado Federal.

[5] Como veremos com mais detalhes no item 2, a União Europeia recentemente adotou um modelo aprimorado de proteção de dados, consubstanciado no Regulamento nº 679 de 2016, que substitui a norma anterior, esta que foi fonte de inspiração para outros ordenamentos jurídicos, a Diretiva nº 95/46/CE.

se deve às interessantes variações e contrastes estratégicos entre cada um: um modelo tradicional, de grande influência para outros países e baseado em uma abordagem personalista; um segundo modelo, diametralmente oposto, baseado em valores como propriedade e liberdade contratual; e um terceiro, que buscou adaptar o modelo europeu às exigências da América Latina da virada do milênio. Esperamos que tal esforço possa evidenciar, em uma análise atenta posterior, quais estratégias regulatórias têm mais sucesso e como elas podem ser combinadas para produzir um paradigma eficiente e prático para garantir a privacidade do indivíduo comum, sem descuidar do incentivo à inovação e ao desenvolvimento tecnológico.

O Modelo Europeu

A União Europeia sempre esteve na vanguarda no que diz respeito à proteção de dados pessoais. A Convenção nº 108 do Conselho Europeu, a chamada Convenção de Estrasburgo, inaugurou[6], em 1981, as iniciativas para um modelo robusto de tutela, que hoje é referência em todo o mundo[7].

Antes que se dê mais um passo, é importante esclarecer sobre a natureza jurídica das normas da União Europeia. Regulamentos são normas vinculativas diretamente aplicáveis a todos os países, incluindo-se aí seus cidadãos e pessoas jurídicas, valendo como se direito nacional fosse. Diretivas são normas adotadas pela Comissão e pelo Parlamento Europeu que fixam um objetivo que todos os Estados-Membros devem alcançar, cabendo a cada um decidir os meios exatos para tal, respeitando os preceitos básicos da norma supranacional. Decisões são atos vinculativos apenas para partes específicas, sejam elas Estados ou empresas, sendo diretamente aplicáveis para os envolvidos. Recomendações e pareceres são atos não vinculativos e podem ser emitidos por diversas instituições europeias, contendo normalmente a recomendação de se adotar ou evitar certa posição ou comportamento, ou a declaração de uma posição quanto à determinada questão[8].

---

[6] Isso sem contar ainda algumas leis anteriores de países daquele continente, por vezes de alcance nacional e por outras leis regionais. Bons exemplos são a Bundesdatenschutzgesetz, de 1977 do Land de Hesse, na Alemanhã, e a Loy Informatique et Libertés, de 1978, da França.

[7] Países como Uruguai, Argentina e Brasil possuem leis de proteção de dados, ou projetos de leis, inspirados profundamente no modelo europeu da Diretiva nº 95/46/CE, a normativa central em vigor no continente.

[8] Os atos jurídicos normativos da União Europeia estão descritos no artigo 288 do Tratado sobre o Funcionamento da União Europeia (TFUE). O TFUE resultou da alteração do Tratado de Roma, de 1957, que estabeleceu a Comunidade Europeia, pelo Tratado de Lisboa assinado em 2007, que reforma os tratados base da

a. Estrutura normativa e de tutela

O sistema[9] atualmente vigente de proteção de dados pessoais é composto por diretivas, regulamentos, decisões vinculantes e orientações de diversos níveis hierárquicos, criando um quadro legal de diversas camadas, que partem sempre de orientações gerais e estabelecem normas cada vez mais específicas sobre os direitos e obrigações relativos aos dados pessoais.

Ainda em vigor[10], a Diretiva 95/46/CE é o texto legal central no sistema europeu de proteção de dados pessoais. A Diretiva centraliza os principais conceitos no campo da proteção dos dados pessoais na União Europeia. Ela traz os princípios básicos da tutela dos dados pessoais, tanto na coleta, quanto na manipulação e tratamento de tais dados pelos interessados e por terceiros, direitos básicos dos titulares dos dados tratados, estabelece padrões para as transferências internacionais de dados e cria ainda um aparato de supervisão que sirva como fiscal, árbitro e legislador, nas funções que a Diretiva lhe atribui.

Outras diretivas, de caráter complementar, foram também criadas, buscando a transposição dos princípios da Diretiva 95/46 para outras áreas de controle antes não abrangidas pelo sistema. O Regulamento nº 45/2001[11], por exemplo, é a norma autoaplicável que vincula as instituições e órgãos da União Europeia a um sistema baseado na Diretiva 95/46/CE para a proteção de dados, ainda que de modo mais detalhado decorrente da necessidade de aplicação direta da norma.

Já a Diretiva 2002/58/CE[12], do Parlamento Europeu e do Conselho, rege o

---

União e reorganiza suas instituições.

[9] Falamos aqui de sistema pois o modo de interrelação entre as diversas Diretivas, Regulamentos, Decisões vinculantes regionais e suas contrapartes nacionais enquadram-se no conceito de Norberto Bobbio, que assim define sistema: "Diz-se que um ordenamento jurídico constitui um sistema porque não podem coexistir nele *normas incompatíveis*. Aqui, "sistema" equivale à validade do princípio que exclui a incompatibilidade das normas. Se num ordenamento vêm a existir normas incompatíveis, uma das duas ou ambas devem ser eliminadas. Se isso é verdade, quer dizer que as normas de um ordenamento têm um certo relacionamento entre si, e esse relacionamento é o relacionamento de compatibilidade, que implica a exclusão da incompatibilidade." BOBBIO, Norberto. **Teoria do ordenamento jurídico**. São Paulo: Polis, 1989. p. 80.

[10] Em 14 de abril de 2016 foi aprovado o Regulamento nº 679/2016, conhecido como Regulamento Geral de Proteção de Dados ou *General Data Protection Regulation (GDPR)*, que substitui a Diretiva nº 95/46. Tal regulamento, por uma questão de adaptação do mercado, só entra em vigor em 25 de maio de 2018.

[11] UNIÃO EUROPEIA. Regulamento (CE) nº 45/2001 do Parlamento Europeu e do Conselho de 18 de dezembro de 2000 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. **Jornal Oficial** L. 008, 12 de janeiro de 2001.

[12] Posteriormente complementada e atualizada pelas Diretivas 2006/24/CE e 2009/136/CE. UNIÃO

tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas. A diretiva aborda questões específicas e sensíveis como a conservação de dados de conexão para fins de faturamento dos serviços de conexão prestados, o envio de mensagens eletrônicas não solicitadas (spam), a utilização de dados pessoais em listagens públicas (como listas telefônicas), e a utilização dos chamados "testemunhos de conexão" ou cookies.

A Diretiva 2006/24/CE[13] complementa o quadro estabelecido, dispondo especificamente sobre a obrigação dos provedores de serviços de comunicação de reter dados de conexão relativos a comunicações levadas a cabo por meio de redes públicas, com especial menção à Internet. Em abril de 2014, no entanto, a Corte de Justiça da União Europeia declarou essa diretiva inválida[14] ao considerar que, enquanto a obrigação de retenção de certos dados de conexão não viola, per se, direitos fundamentais da Carta de Direitos, o modo como é determinada a retenção é desproporcional.

Um degrau abaixo das diretivas e regulamentos, encontramos algumas decisões da Comissão Europeia que ajudam a complementar o quadro regulatório. Essas decisões, não sendo produto de deliberações generalizadas[15] - como no caso dos regulamentos e diretivas sobre o assunto, que precisam ser aprovadas pelo Parlamento Europeu -, são mais facilmente revistas e atualizadas, característica que permite um detalhamento ainda maior em suas provisões.

Uma das mais famosas decisões foi a Decisão da Comissão 2000/520/EC, datada de

---

EUROPEIA. Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações electrónicas. **Jornal Oficial** L. 201, 31 de julho de 2002.

[13] UNIÃO EUROPEIA. Directiva 2006/24/CE do Parlamento Europeu e do Conselho de 15 de março de 2006 relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Diretiva 2002/58/CE. **Jornal Oficial** L. 105, 13 de abril de 2006.

[14] UNIÃO EUROPEIA. Corte de Justiça da União Europeia, Casos conjuntos C-293/12 e C-594/12. **Digital Rights Ireland Ltd. v. Ireland**, julgados em 8 de abril de 2014. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?docid=150642&mode=req&pageIndex=1&dir=&occ=first &part=1&text=&doclang=PT&cid=513860>. Acesso em: 09.10.14.

[15] Segundo o artigo 16, 2 do TFUE, o Parlamento Europeu e o Conselho da União Europeia devem adotar o processo legislativo ordinário para dispor sobre a proteção dos cidadãos quanto ao tratamento de seus dados pessoais. Por tal procedimento, de acordo com os artigos 289 e 294 do mesmo tratado, a proposta de normativa (regulamento, diretiva ou decisão) é introduzida pela Comissão Europeia e encaminhada para análise do Parlamento e do Conselho, que proferem ao fim uma decisão conjunta. Em alguns casos, no entanto, a Comissão pode emitir decisões únicas, quando assim autorizado por norma não obstada pelo Parlamento ou pelo Conselho, conforme o artigo 290 do TFUE. No caso, a própria Diretiva 95/46/CE delega à Comissão a regulamentação de alguns pontos específicos através de decisões únicas, como é o caso do artigo 24, item 6, e do artigo 25, item 4.

26 de julho de 2000, que dizia respeito a um programa de "porto seguro"[16], criado em conjunto com o Departamento de Comércio dos Estados Unidos da América[17], para facilitar as transferências de dados pessoais entre as duas partes, pelo estabelecimento de padrões mínimos de segurança e sigilo. Entre as razões para sua concretização, estava o fato de que a União Europeia via com grande preocupação o cenário legislativo norte-americano no que tocava a proteção de dados pessoais, uma vez que, sendo os Estados Unidos um grande polo empresarial e principalmente no oferecimento de produtos e serviços em um ambiente *online*, havia a legítima preocupação sobre o destino dos dados de cidadãos europeus eventualmente transferidos a empresas localizadas naquele país. O programa "Safe Harbor" foi encerrado em outubro de 2015, quando a Corte de Justiça da União Europeia, diante das denúncias feitas pelo ex-agente da Agência de Segurança Nacional norte-americana (NSA), Edward Snowden[18], sobre violações generalizadas de privacidade pelo governo estadunidense, julgou inválida a Decisão 2000/520/CE.

Na sequência dessa decisão, entabularam-se novas discussões entre Estados Unidos e União Europeia, a fim de criar um novo programa para garantir o intercâmbio de informações. O resultado desses esforços foi a Decisão de Execução 2016/1250/CE[19], que estabeleceu o agora conhecido programa "Privacy Shield", que aprimorou o programa anterior[20]. O programa, no geral, exige que as empresas afiliadas garantam certos direitos aos indivíduos cujos dados são transferidos, como informações básicas, acesso a mecanismos simples e gratuitos de resolução de disputas, além de exigir o cumprimento de alguns princípios básicos de proteção de dados, sigilo e segurança dos dados e a transparência no tratamento dos mesmos.

É também de grande interesse a Decisão da Comissão 2001/497/CE, datada de 15 de

---

[16] "Safe Harbour"

[17] COMISSÃO EUROPEIA. Decisão 2000/520/CE. Decisão da Comissão de 26 de julho de 2000 nos termos da Directiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípio de "porto seguro" e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América. **Jornal Oficial L** 215, 25 de agosto de 2000.

[18] GREENWALD, G.; MACASKILL, E. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian Online**, June 7, 2013. Disponível em: <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 30.11.16.

[19] UNIÃO EUROPEIA. Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. **Jornal Oficial** L. 207/1, 01 de agosto de 2016.

[20] A adesão ao programa Privacy Shield é voluntária, apesar de ser requisito para transferências de dados que envolvam a União Europeia. Uma vez feita a adesão ao programa, no entanto, o atendimento a seus requisitos é obrigatório e exigível pela lei local norte-americana. Para mais informações, confira-se: https://www.privacyshield.gov/.

junho de 2001[21], que fornece aos interessados em transferir dados pessoais para destinos externos à União Europeia cláusulas-tipo que apresentam garantias suficientes, nos termos da Diretiva 95/46/CE, para a preservação dos direitos concedidos por aquela diretiva aos titulares dos dados a serem transferidos.

A comprovar a flexibilidade desse tipo de normativa, apenas 3 anos após a publicação da Decisão 2001/497/CE, a Comissão emitiu nova decisão sobre o assunto, publicada em 27 de dezembro de 2004[22], alterando alguns poucos dispositivos da decisão anterior e introduzindo um novo conjunto de cláusulas típicas, que poderiam ser combinadas ou utilizadas em substituição ao primeiro conjunto, consignado na primeira decisão.

Este sistema bem conhecido e consolidado de normas sofreu grande alteração em 2016, quando foi aprovada uma grande reforma, gestada desde 2010[23]. A reforma se deu, sobretudo, pela introdução do Regulamento nº 679/2016 do Parlamento e do Conselho, que substitui a Diretiva nº 95/46/CE e unifica a disciplina da proteção dos dados pessoais, uma vez que é diretamente aplicável como se norma interna fosse, reduzindo também a fragmentação do sistema ao não ser mais necessária a incorporação do texto supranacional por uma lei interna. Tal regulamento ficou conhecido como o Regulamento Geral de Proteção de Dados[24],o *General Data Protection Regulation* ou, simplesmente, GDPR[25].

Entre as principais alterações trazidas pelo GDPR, temos sete que são mais

---

[21] COMISSÃO EUROPEIA. Decisão 2001/497/CE. Decisão da Comissão de 15 de junho de 2001 relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros, nos termos da Directiva 95/46/CE. **Jornal Oficial L** 181, 4 de julho de 2001.

[22] COMISSÃO EUROPEIA. Decisão 2004/915/CE. Decisão da Comissão de 27 de dezembro de 2004 que altera a Decisão 2001/497/CE no que se refere à introdução de um conjunto alternativo de cláusulas contratuais típicas aplicáveis à transferência de dados pessoais para países terceiros. **Jornal Oficial L** 385, 29 de dezembro de 2004.

[23] COMISSÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões. Uma abordagem global da protecção de dados pessoais na União Europeia. Bruxelas, 4 nov. 2010. COM(2010) 609 final. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pt.pdf>. Acesso em: 24.03.17.

[24] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à protecção 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). **Jornal Oficial** L. 119/1008, 04 de maio de 2016.

[25] Juntamente ao GDPR foi também aprovada a Diretiva nº 2016/680/CE, que regula o tratamento de dados pessoais no contexto da investigação, repressão e persecução criminais pelas autoridades competentes, mas que não nos interessa diretamente no presente estudo. Confira-se: UNIÃO EUROPEIA. Diretiva (UE) nº 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. **Jornal Oficial** L. 119/89, 04 de maio de 2016.

relevantes, que por sua vez podem ser divididas por sua finalidade: alterações para reforçar direitos dos usuários, alterações para reforçar as competências das Autoridades de Proteção de Dados, e alterações para *induzir* e *incentivar* certos comportamentos por parte dos responsáveis pelo tratamento.

Em primeiro lugar, no que toca o reforço dos direitos individuais, a forma de expressão do consentimento e a relevância do adjetivo "informado" foram reforçados, exigindo-se que o titular dos dados tenha acesso facilitado às informações sobre o tratamento, expressas de modo simplificado (ao invés da linguagem geralmente hermética dos contratos), e que seu consentimento seja expressado de modo destacado, com igual facilidade para sua revogação. Ainda para reforçar direitos dos titulares, os direitos de acesso e de eliminação de dados (na forma do "direito ao esquecimento"), são reelaborados e expandidos, dando maior segurança ao titular e ao mercado.

No que toca o reforço das Autoridades de Proteção de Dados, podemos citar a especificação de sanções que podem ser impostas aos responsáveis por tratamentos de dados que não respeitem as regras do GDPR, a responsabilização também do agente processador dos dados e a nova obrigação de notificação de violações de segurança de dados. Assim, empresas que sofrerem ataques para roubo de dados ou que tiverem dados pessoais de seus clientes vazados, por exemplo, deverão agora notificar os titulares dos dados e a Autoridade de Proteção de dados sobre tal fato. Ainda nessa esteira, o novo Regulamento cria diversas regras sobre procedimentos de avaliação de impacto em privacidade, os chamados *Privacy Impact Assessments*, ou simplesmente PIAs. Apesar de não haver uma obrigação de registro de tratamentos de dados, em certos casos é exigido do controlador ou responsável que elabore tal estudo, de modo a reduzir os riscos à privacidade dos titulares dos dados, podendo submetê-lo à aprovação da Autoridade de controle.

Por fim, o Regulamento traz também algumas práticas que servem como incentivo ao responsável pelo tratamento dos dados pessoais, para que este zele pelo cumprimento do regulamento e pela garantia da privacidade dos titulares dos dados. A primeira mudança vem pela consolidação dos conceitos de *privacy by default* e *privacy by design* como obrigações do responsável pelo tratamento, pelo que deve sempre construir seus produtos, serviços e processos tendo em mente a preservação da privacidade e os princípios gerais da matéria, além de utilizar como padrão de operação a escolha pela preservação da privacidade em detrimento da publicidade, na ausência de um posicionamento expresso do titular dos dados.

A segunda mudança, de igual importância, vem pela reafirmação dos programas de incentivo ao cumprimento do Regulamento pela criação de selos e sistemas de certificação relacionados ao grau de zelo da empresa com a privacidade de seus usuários.

b. Tutela em camadas, indução de comportamentos e fiscalização multinível

O que se nota pelo panorama traçado é um sistema de proteção construído em camadas: partimos de garantias fundamentais de grande amplitude, passando a normas ainda bastante gerais que especificam tais princípios e preveem tanto exceções quanto possíveis conflitos com outros princípios, e em seguida ainda a novas normas ainda mais específicas que abordam questões setoriais, por fim chegando a decisões e normativas de ainda maior especificidade, mas que contam com grande flexibilidade em sua criação e atualização.

Nessa estrutura piramidal os valores essenciais estão contidos no topo, em normas gerais de pouca aplicabilidade prática e direta, crescendo os instrumentos legais em número, especificidade e flexibilidade conforme avançam para a base da estrutura.

Essa configuração é de imensa importância diante das dificuldades inerentes à regulação de um setor tão influenciado pelo desenvolvimento tecnológico, como é o caso dos dados pessoais[26]. O importante, a essa altura, é perceber que essa estrutura hierarquizada de valores, princípios e regras é essencial por um fator crucial: a sincronia entre a lei e a realidade. Em um campo fático de rápida evolução, é importante que a lei mantenha um patamar mínimo de aplicabilidade e sejam, no mais, envidados esforços para a atualização constante das normas, de modo que estas possam acompanhar - ainda que a certa distância - o desenvolvimento tecnológico.

Estruturadas como se encontram, as normas comunitárias básicas sobre a proteção de dados fornecem uma estrutura onde (i) os valores fundantes - cuja atualização não precisa seguir o ritmo da tecnologia - estão bem fixados em normas gerais, que costumam apresentar também maiores dificuldades para sua alteração; (ii) os princípios e subprincípios em que se traduzem tais valores são bem desenhados e fixados em normas ainda de caráter geral, mas tecnologicamente neutras - o que garante que possam ser aplicadas ainda que com mudanças razoáveis no campo tecnológico; e (iii) regras específicas criadas pelo sopesamento e fixação

[26] MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with technology as a regulatory target. **Law, Innovation and Technology**, n. 5, v. 1, 2013.

legal desses princípios, são erigidas em normas de caráter específico e sujeitas a um procedimento simplificado de produção e atualização - permitindo que, ainda que não absolutamente tecnologicamente neutras, sigam a curta distância o desenvolvimento tecnológico.

Do ponto de vista regulatório, a garantia de certos direitos e a condução dos atores envolvidos a um "comportamento ideal" é buscada por vias diferentes, que se complementam. Por um lado, temos princípios gerais e normas de conduta que impõem certos deveres. Por outro, temos também o recurso a práticas de mercado, como a autorregulação e a criação de sistemas que premiam o cumprimento da lei, mais que simplesmente punir sua violação. Ainda, contamos no modelo europeu com a importante figura das Autoridades de Proteção de Dados, cujas atribuições extrapolam o de uma simples agência reguladora, mas caracterizam um órgão que agrega funções fiscalizatórias, normativas e jurisdicionais, ainda que em uma instância administrativa. Esse último ponto permite que os titulares de dados possam acompanhar de perto o que é feito de seus dados e tenham um canal efetivo e especializado para a resolução de controvérsias que possam surgir, incentivando assim que o próprio usuário seja um fiscal ativo de seus direitos.

O Modelo Norte-americano

O segundo modelo regulatório a ser examinado é o vigente nos Estados Unidos. O modelo norte-americano é o segundo mais influente do mundo, sendo que a maioria dos estudiosos define que, na atualidade, geralmente a lei de proteção de dados pessoais recentemente adotada (ou a tutela dos dados em sua ausência) tem grande chance de adotar um dos dois sistemas, ou neles se inspirar[27].

a. Estrutura normativa e de tutela

Os Estados Unidos não possuem uma lei geral de proteção de dados pessoais no âmbito federal. Em lugar de tratar a disciplina da coleta e do uso dos dados pessoais de uma

[27] "The United States, which long supported market-based solutions, rejected the legitimacy of the EU's legislation, stoking the first trade conflict of the information age.(...) Against U.S. objections, European rules became the *de facto* international standard with more than thirty countries following the European approach." NEWMAN, Abraham L. Building transnational civil liberties: transgovernmental entrepreneurs and the European data privacy directive. **International Organization**, n. 62, n. 1, p. 104, Jan. 2008. Confira-se também: CASTETS-RENARD, Céline. **Droit de l'internet: droit français et européen**. 2.ed. Paris: Montchrestien, 2012. p. 26.

maneira uniforme, optou-se por dar um tratamento setorial à matéria. Desse modo, o país possui leis federais que disciplinam a proteção e o uso de dados pessoais de crianças e adolescentes, os dados médicos ou de saúde, os dados financeiros, os dados pessoais inseridos no contexto das comunicações eletrônicas, entre outros setores específicos, mas não há uma lei central que defina princípios e regras comuns, ou que estabeleça direitos unificados aos cidadãos. Alguns estados também possuem legislação específica sobre privacidade e proteção de dados, devendo-se destacar o exemplo da Califórnia, que é uma das referências naquele país no tema[28].

Uma das leis mais interessantes no âmbito federal é o *Electronic Communications Privacy Act* de 1986[29], que é constituído do *Wiretap Act*, o *Stored Communications Act* e o *Pen Register Act*. O *Wiretap Act* proíbe a interceptação, uso ou revelação de qualquer tipo de comunicação telefônica, oral ou eletrônica, aplicando-se tanto ao setor privado quanto ao público (salvo as exceções em caso de investigação criminal, por exemplo). Note-se que a referência aqui é a comunicação *em fluxo*, o que se extrai do próprio termo *interceptação*. Os dados referentes a comunicações armazenadas, que já foram recebidas ou enviadas e não se encontram mais em fluxo, são protegidos, por sua vez, pelo *Stored Communications Act*, que diz respeito aos dados de comunicação e de cadastro (como nome, endereço, etc) armazenados por provedores de serviço. O *Pen Register Act* regula a utilização pelo governo (e a proibição ao público em geral) dos *pen registers* e outros dispositivos de rastreamento de chamadas. Esses dispositivos servem para identificar os terminais em uma determinada comunicação (geralmente telefônica), mas não tem capacidade para interceptar ou acessar o conteúdo da comunicação em si.

Ainda no âmbito federal, o COPPA, acrônimo para *Children's Online Privacy Protection Act*[30], lei de 1998 que cria salvaguardas para a interação de crianças com menos de 13 (treze) anos com a Internet em geral e no que diz respeito a sua privacidade. A Lei traz um mecanismo interessante de *safe harbor*, diferente do projeto internacional entre Estados Unidos e União Europeia. Por tal mecanismo, associações setoriais de empresas podem submeter à *Federal Trade Comission* (FTC) códigos de auto regulação que serão então

[28] SOTTO, L.J.; SIMPSON, A.P. United States In: **Data Protection & Privacy 2015**, Londres: Law Business Research, 2015, pp. 208-209.
[29] ESTADOS UNIDOS DA AMÉRICA. Electronic Communications Privacy Act, 18 U.S.C. §2510 e ss., **Public Law**, Washinton D.C., 21 out. 1986.
[30] ESTADOS UNIDOS DA AMÉRICA. Children's Online Privacy Protection Act, 15 U.S.C. §6501-6506., **Public Law**, Washinton D.C., 21 out. 1998.

avaliados e eventualmente homologados, tornando-se vinculantes para as empresas associadas. O diferencial aqui diz respeito ao fato de que tais códigos geralmente preveem mecanismos de resolução de disputas entre as empresas associadas e seus consumidores e/ou mecanismos internos de disciplina das empresas envolvidas em possíveis violações de privacidade. Com tais provisões, uma vez aprovado o código, empresas em violação do COPPA estariam primeiro sujeitas aos procedimentos disciplinares setoriais, e só depois, em certos casos, poderia ser submetidas à investigação da FTC.

No setor da saúde, vige o *Health Insurance Portability and Accountability Act* de 1996, mais conhecido por *HIPAA*, que traz regras federais setoriais de privacidade e proteção de dados médicos[31]. Tal lei traz disposições padrões de segurança, física e técnica, para dados relacionados à saúde em formato eletrônicos; a obrigação de notificar os titulares dos dados, e muitas vezes a Secretaria de Saúde[32] e a mídia local[33] no caso de vazamento ou violações de dados pessoais; as condições básicas para o tratamento justo e legal dos dados pessoais e as situações em que o consentimento do titular é ou não necessário; direitos básicos de acesso aos dados e informação sobre o tratamento e as cabíveis medidas de segurança e sigilo; além de diretrizes específicas sobre a responsabilidade da "entidade abrangida" pela lei por seus funcionários, incluindo-se aí treinamentos, questões de política interna de privacidade e disciplina.

O *Privacy Act* de 1974[34] é a lei federal vigente que estabelece os princípios e regras para a coleta, armazenamento, uso e comunicação de dados pessoais no seio das atividades estatais conduzidas pelas agências federais. A lei traz regras sobre a revelação de dados pessoais a outras agências ou terceiros, geralmente mediante o consentimento do titular ou diante de alguma circunstância de interesse público - no exercício da administração pública ou em atividades particulares com fins estatísticos, históricos, negocial, entre outros - ; garante direitos de acesso; limitações quanto à finalidade, quantidade e qualidade dos dados tratados; diretrizes para garantir a segurança, sigilo e a transparência dos tratamentos; diretrizes sobre as políticas internas de segurança e tratamento de dados; a obrigatoriedade de registro dos bancos de dados federais submetidos ao *Privacy Act*, entre tantos outros assuntos

[31] ESTADOS UNIDOS DA AMÉRICA. Health Insurance Portability and Accountability Act, 110 Stat. 1936, **Public Law**, Washinton D.C., 21 ago. 1996.
[32] U.S. Department of Health and Human Services.
[33] Quando o número de indivíduos afetados superar 500 (quinhentos) em um mesmo estado.
[34] ESTADOS UNIDOS DA AMÉRICA. Privacy Act, 88 Stat. 1896, **Public Law**, Washinton D.C., 31 dez. 1974.

menores.

O sistema estadunidense não possui uma Autoridade de Proteção de Dados nos moldes europeus, um órgão técnico, independente e dedicado unicamente à matéria da privacidade e da proteção de dados pessoais. Em seu lugar, certos órgãos já existentes e não exclusivos do governo atuam como agências reguladoras, sendo responsáveis pelo *enforcement* das leis vigentes, igualmente separados por setores econômicos, de modo que sua atuação não é necessariamente homogênea, como também não são necessariamente suas posições em relação às controvérsias que possam surgir sobre este ou aquele conceito. Assim, a *Federal Trade Commission* é responsável, por exemplo, por fiscalizar a aplicação do COPPA e das regras relativas à proteção do consumidor, segundo seu próprio estatuto[35], que podem incluir abusos na coleta e utilização de dados dos consumidores. Já o *Department of Health and Human Services*, é responsável pela supervisão do cumprimento do HIPAA. No setor financeiro, temos o *Consumer Financial Protection Bureau*.

Tais agências geralmente têm competências fiscalizatórias, sancionatórias e normativas, podendo complementar as regras setoriais de que cuidam, mas o Poder Judiciário ainda exerce um importante papel no sistema de tutela. Mesmo tais agências e escritórios geralmente precisam recorrer ao Judiciário para executar suas decisões ou buscar o cumprimento de certas obrigações, o que demonstra a posição central do processo judicial no sistema. Não bastasse tal, na ausência de leis mais amplas de proteção de dados, os princípios e regras gerais necessários para um modelo mais completo de tutela geralmente têm que ser deduzidos dos precedentes judiciais, reafirmando sua importância.

b. Descentralização, contratualismo e judicialização

O modelo regulatório dos Estados Unidos é único na medida que apresenta uma abordagem bastante heterodoxa no que toca às limitações à proteção de dados. Há de fato o reconhecimento de que os dados pessoais têm alguma ligação com a privacidade do indivíduo e com o controle que esse exerce sobre sua vida particular[36]. Tal "direito à tutela", no entanto, dificilmente é autoaplicável ou diretamente exigível pelo titular dos dados daquele que os coleta e os trata.

---

35 ESTADOS UNIDOS DA AMÉRICA. Federal Trade Comission Act, 15 U.S.C. §41-58., **Public Law**, Washinton D.C., 1914.

36 WESTIN, Alan. Privacy and Freedom, New York: Atheneum, 1970 *apud* PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. 1. ed. 6. imp, Curitiba: Juruá, 2011, p. 128.

A norma de direito mais próxima do indivíduo é, pois, o contrato que rege sua relação com a empresa que coleta e utiliza seus dados pessoais. Talvez por conta da alta estima em que tem a liberdade, o legislador parece deixar à liberdade das partes de contratar a definição do que é razoável e possível. O instituto central do modelo norte-americano pode ser apontado, pois, como o *consentimento*. As condições e características desse consentimento variam de acordo com o setor de mercado e com a corte competente, mas é bastante claro que o consentimento possui, no contexto norte-americano, valor muito maior que aquele a ele atribuído nos demais modelos regulatórios, pois não se trata aqui de um *consentimento informado*, livre ou expresso, *resultado da consideração do indivíduo sobre o que se pretende com seus dados* e o sopesamento entre benefícios e malefícios. O consentimento, na tradição norte-americana, parece ter maior ligação com a *venda* de informações que com o estabelecimento de uma relação entre o usuário e o responsável pelo tratamento, dando-se ao contrato o tom de uma transação comercial, ao invés de uma cessão temporária de direitos sobre os dados em questão[37].

O contrato, no entanto, não serve sempre como substituto à garantia de certos direitos abrangentes. Principalmente em situações em que uma das partes é uma grande empresa e a outra um indivíduo que deseja usufruir de um serviço seu – ao qual não terá acesso caso não aceite o contrato padrão provedor do serviço – o usuário vê-se forçado a aceitar termos impostos pelo provedor, não importa quão injustos. Esse desequilíbrio contratual, resultado da disparidade de força das partes, gera situações abusivas que não são tuteladas pela lei e, pela massificação dos negócios digitais[38], por sua vez acarretam ações judiciais, individuais ou coletivas, como única solução.

A judicialização de conflitos, ampliada pela ausência de uma norma geral ou mesmo de um órgão regulador específico, tem diversas consequências, tanto para a efetividade dos direitos garantidos quanto para a condução dos negócios em si.

Por um lado, temos que determinada situação considerada lesiva aos interesses de uma das partes é colocada sob exame de uma autoridade judicial que, ainda que não seja

---

[37] "In contrast to other areas of the world such as the United States, where personal information is widely traded like a conventional good, European rules limited the commodification of individual data." NEWMAN, Abraham L. op. cit., p. 104.

[38] Confira-se, por exemplo: BARRETT, Brian. Spotify clears up its controversial Privacy Policy. **Wired Online**, 21 ago. 2015. Disponível em: <https://www.wired.com/2015/08/spotify-clears-up-its-privacy-policy/>. Acesso em 19.01.17. PAUL, Ian. Instagram updates Privacy Policy, inspiring backlash. **PC World.** 18 dez. 2012. Disponível em: <http://www.pcworld.com/article/2021285/instagram-updates-privacy-policy-inspiring-backlash.html>. Acesso em 19.01.17.

especialista no assunto em tela, tem por delegação o poder estatal para dar solução definitiva ao litígio, garantindo a observância da lei tanto no curso do procedimento quanto na execução do provimento. Por outro, consigna-se a solução de um litígio técnico, e que exige rápida resposta, a uma entidade que não possui o conhecimento técnico muitas vezes necessário e cujo prazo mínimo para atingir um primeiro provimento definitivo é grande demais, a ponto de ser totalmente ineficaz do ponto de vista fático.

Afirmamos isso pois a maioria esmagadora dos dados pessoais em circulação advém e tem como seu contexto a Internet e outros sistemas informatizados, geralmente conectados em rede, e o tempo entre as transações, ações de tratamento, comunicação de dados, é infinitamente menor ao usual, dentro do qual uma solução judicial seria viável.

Em um segundo aspecto, temos, no foco da nossa análise, uma consequência mais ampla relacionada ao comportamento das partes desde a concepção de um modelo de negócio até seu efetivo fornecimento. Relegar ao judiciário a garantia de direitos, sem criar outros mecanismos que garantam direitos ou busquem incentivar a adoção de certas práticas de bom tom no tratamento da privacidade dos indivíduos, instila no empreendedor e nas empresas em geral a ideia de que a garantia da privacidade de seus clientes ou futuros clientes é apenas um fator na análise de rentabilidade e viabilidade de um modelo de negócios, e não um valor que deve ser preservado.

Do ponto de vista geral, essa abordagem privilegia a livre iniciativa e a inovação, permitindo que usos novos e não regulados da informação sejam descobertos e utilizados para gerar valor aos consumidores. Do ponto de vista da proteção de dados pessoais, no entanto, trata-se de um modelo ineficaz de regulação, que recorre apenas a um viés regulatório jurídico, ao invés de avaliar a conduta regulada em termos econômicos, sociais e de "arquitetura", como queria Lessig.[39] Vale, nesse ponto, considerar se a via adotada pelos juristas estadunidenses é a única e mais efetiva alternativa para realizar os dois propósitos aparentemente contraditórios: privacidade e livre iniciativa[40].

---

[39] LESSIG, Lawrence. **Code version 2.0**. [S.l.]: Lawrence Lessig C.C., Kindle Edition, 2011. pos. 1536-1545. ASIN: B004NNVWEI.

[40] De uma parte: "A ideia de consentimento do afetado, cujo estágio temporal é necessariamente após a noção de *informação* anteriormente tratada, é tão central ao modelo europeu de proteção de dados, que um dos maiores e mais antigos estudiosos espanhóis sobre o tema afirmou em uma de suas obras que esse 'es la piedra angular a partir del cual se construye el sistema de protección de datos personales'" SILVA, Carlos Bruno Ferreira da. **Proteção de Dados e Cooperação Transnacional,** Belo Horizonte: Arraes, 2014, p. 187. De outra parte, confira-se: "De una parte, argumentamos que, en cuanto expediente legitimador y forma de protección del titular de los datos, el consentimiento es un mecanismo inadecuado: la concepción "individualista" que subyace a este enfoque protector no sirve en un mundo de computación ubicua donde las prácticas de obtención y análisis

O Modelo Uruguaio

O modelo regulatório uruguaio é de especial interesse para nós pois a preocupação com a privacidade de dados dos cidadãos naquele país teve origem semelhante à brasileira, na medida em que ambas foram resultado de uma tradição sul-americana de reafirmação e expansão de direitos fundamentais, após regimes ditatoriais que tiveram na compilação de dados sobre seus cidadãos, principalmente aqueles de ideais incompatíveis com tais regimes, uma importante arma na repressão de movimentos democráticos[41].

a. Estrutura normativa e de tutela

A principal lei uruguaia no tema é a Lei nº 18.331 de 2008 que trata da "Proteção de dados pessoais e da ação de 'Habeas Data'"[42], representando o ponto central do sistema de tutela daquele país. A referida lei traz as disposições gerais aplicáveis a todos os contextos onde dados pessoais possam ser coletados, tratados e utilizados. Especificamente, a lei traz disposições sobre princípios gerais da proteção de dados; os direitos de informação, acesso, retificação, supressão a dados, proteções especiais para categorias de dados consideradas sensíveis; algumas disposições específicas sobre a utilização de dados pessoais em setores como publicidade, bancos de dados de consumo e telecomunicações; regras para transferências internacionais de dados; registro obrigatório de bancos de dados; a criação do

masivo de datos son inevitables y banalizan la idea del tratamiento "consentido". De otra parte, sostenemos que el discurso oficial del control individual de la información personal ligado a esa idea – al que parece aferrarse aún la futura normativa europea – ha acabado convertido en una suerte de letanía que a duras penas se refleja en la práctica y que predica de la legislación de protección de datos un poder para conformar la realidad social que no tiene." OLIVER-LALANA, A.D.; SORO, J. F. M. El mito del consentimiento y el fracaso del modelo individualista de protección de datos, *In:* TORRIJOS, J. V. (org). **La Protección de los Datos Personales en Internet ante la Innovación Tecnológica**, Navarra: Aranzadi, 2013, pp. 153-196. A respeito dessa discussão, confira-se também: BENNETT, Colin J. **Regulating Privacy: Data Protection and Public Policy in Europe and the United States**, Ithaca: Cornell University Press, 1992, pp. 193-219.

[41] "Sinteticamente, apontamos o fato de que um instituto do gênero tenha uma especial razão de ser em sociedades recém-saídas de regimes ditatoriais, como era o panorama em muitos países latino-americanos na década de 1980 em diante, em cuja sociedade civil persistia o trauma pelo uso autoritário da informação. Em um momento posterior ao fim destes regimes, um instrumento para a requisição das informações pessoais em mãos do poder público, em particular pelos órgãos diretamente encarregados pela repressão à atividades insurrecionais, era tanto desejado quanto necessário, seja para a tutela dos direitos fundamentais envolvidos como também pelo seu importante papel na formação de uma cultura democrática. Com tal escopo foi concebido o *habeas data* - para proporcionar, portanto, ao cidadão um instrumento para conhecer diretamente e, se necessário, retificar as informações sobre sua própria pessoa armazenadas em bancos de dados [de caráter público]." DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 327-328.

[42] URUGUAI. Lei nº 18.331 de 2008 sobre a Proteção de dados pessoais e a ação de 'Habeas Data'. **Diario Oficial,** Montevideo, 18 ago. 2008.

Órgão de Controle, chamado "Unidad Reguladora y de Control de Datos Personales", que consiste, basicamente, em uma Autoridade de Proteção de Dados; e disposições específicas sobre a ação de "Habeas Data", um dos elementos centrais do modelo regulatório.

A Lei nº 18.331 de 2008 foi regulamentada pelo Decreto nº 414 de 2009[43], que trata com maior minúcia alguns temas da Lei de Proteção de Dados. Entre esses temas, podemos citar especificações sobre a comunicação do consentimento para tratamento de dados; medidas técnicas e administrativas de segurança; e detalhes sobre o exercício dos direitos de acesso, retificação e eliminação ou supressão de dados. O decreto não elabora a atribuição normativa do Órgão de Controle, deixando em aberto os temas a serem objeto de tais orientações ou mesmo o peso jurídico de tais documentos.

Algumas outras normativas tratam da coleta e tratamento de dados pessoais em certos setores, como o Decreto nº 396 de 2003, que trata dos dados pessoais referentes à saúde do indivíduo, e o Decreto nº 249 de 2007 que regula a identificação de pessoas por meios informáticos. Por fim, a própria Unidad Reguladora y de Control de Datos Personales emite normativas de caráter particular, interpretando e integrando as regras contidas na legislação vigente sobre Proteção de Dados.

b. Centralização, registro obrigatório e o remédio do Habeas Data

O modelo uruguaio de regulação e proteção de dados pessoais guarda semelhanças com o modelo europeu, mesmo considerando que sua lei geral de proteção tomou sua inspiração da Diretiva 95/46/CE da União Europeia, modelo hoje praticamente ultrapassado, tanto pelo desenvolvimento do sistema uruguaio quando do próprio sistema europeu, com sua recente reforma. Não obstante, algumas diferenças são fundamentais, tanto na adoção inicial quanto nos caminhos adotados em um e noutro contexto.

À semelhança do modelo europeu de proteção de dados, o Uruguai conta com um arcabouço normativo diversificado e estratificado, ainda que não chegue ao nível de complexidade das normas que têm como referência. Encontramos uma lei geral, cujos pontos mais importantes são desenvolvidos com mais detalhes em decretos regulamentadores. Encontramos também normativas emitidas pela Autoridade de Proteção de Dados criada naquela lei geral, a "Unidad Reguladora y de Control de Datos Personales" que regulam assuntos específicos e muitas vezes técnicos, como cláusulas contratuais para transferência

[43] URUGUAI. Decreto nº 414 de 2009. **Diario Oficial,** Montevideo, 31 ago. 2009.

internacional de dados pessoais[44] e monitoramento de ambientes por vídeo[45]. Ainda, paralelamente, temos o incentivo para a adoção de códigos de conduta, que complementa a legislação estatal com a auto regulação dentro dos princípios gerais já estabelecidos.

O tom das normas em vigor, no entanto, não deixa dúvida de que a legislação uruguaia tem forte tendência à centralização de competências. As normativas baseiam-se, antes de tudo, em direitos de acesso, retificação e eliminação de dados, garantidos de modo abrangente, combinado com o registro obrigatório de bases de dados.

Essa configuração permite à Autoridade de Proteção de Dados que realize um controle prévio do tratamento previsto, através da análise de informações como os procedimentos de coleta e tratamento de dados, medidas de segurança e descrição técnica da base de dados, destino dos dados em caso de comunicação, entre outras. A Autoridade pode também, seja através de denúncias, inspeções ou solicitação de informações, fiscalizar o cumprimento da lei, podendo aplicar as sanções administrativas permitidas, quais sejam, advertência, multa ou suspensão de bases de dados.

Uma última característica da Autoridade de Proteção de Dados uruguaia é de grande relevância para o presente mapeamento: a inexistência de competência jurisdicional ou de resolução de conflitos. Ao contrário de modelos como o europeu, a Autoridade uruguaia não tem poder decisório para determinar certa conduta a um ente, público ou privado, que entre em conflito com um cidadão. Ao invés disso, a Autoridade deve informar, ao cidadão que a procure com uma querela, sobre os meios judiciais a sua disposição para buscar a tutela adequada de seus direitos[46]. Não há, pois, uma instância administrativa dedicada a questões relacionadas a proteção de dados, sendo tais casos direcionados ao Poder Judiciário em geral, que pode ser acionado exclusivamente pelo titular dos dados.

Por fim, é necessário notar que o modelo regulatório uruguaio promove a judicialização de conflitos sobre dados pessoais, contando o sistema com um remédio específico, o Habeas Data. Essa ação visa especificamente permitir ao cidadão "tomar conhecimento de dados referentes a sua pessoa, e sua finalidade e usos, que constem em

[44] Confira-se Dictamen nº 003/2009 da Unidad Reguladora y de Control de Datos Personales.

[45] Confira-se Dictamen nº 014/2011 da Unidad Reguladora y de Control de Datos Personales.

[46] É verdade que a Unidad Reguladora y de Control de Datos Personales pode, com base em uma denúncia de violação de um direito garantido em lei, realizar uma inspeção e sancionar a empresa em falta. No entanto, seu provimento será sempre limitado à aplicação de uma das três sanções descritas na lei, não podendo a Autoridade determinar, por exemplo, que a empresa adote determinado comportamento ou tome as providências para garantir determinado direito. A Autoridade de Proteção pode simplesmente autuar as violações da lei, cabendo ao Poder Judiciário qualquer provimento positivo para obrigar a empresa violadora a garantir certo direito.

bancos de dados público ou privados" podendo exigir, segundo o caso, sua retificação, inclusão ou supressão. Na ausência de meios administrativos de solução de controvérsias, salvo a negociação direta com o responsável pelo tratamento ou pela pressão exercida por sanções administrativas da Autoridade de Proteção de Dados em casos coletivos, resta ao cidadão buscar o Poder Judiciário.

Conclusão

Os três modelos regulatórios estudados nos permitem estabelecer alguns pontos em comum e diferenças fundamentais entre diferentes estratégias regulatórias. Os três países estudados não foram escolhidos ao acaso, mas sim por representarem modelos de razoável sucesso na garantia de direitos e, principalmente, por se fiarem em diferentes combinações entre soluções normativas, mercadológicas, sociais e técnicas para atingir seus objetivos. Não se pretende aqui comparar os modelos de modo a apontar o mais adequado. Além de não ser objeto do presente artigo, em razão da extensão de tal tarefa, a indicação de um modelo regulatório como "ideal" contradiz em sua essência qualquer estudo comparativo de ciências sociais aplicadas.

Após a avaliação dos pontos comuns e das diferenças essenciais, podemos então arriscar buscar os contornos de cada uma das três estratégias regulatórias, explicitando seus traços fundamentais.

a. Semelhanças

Os pontos comuns, relevantes para a estratégia regulatória, aos três modelos regulatórios são quatro: (i) a relevância do consentimento, (ii) a obrigação de transparência, (iii) os direitos de acesso, retificação e eliminação de dados, e (iv) as obrigações de segurança e sigilo dos dados pessoais.

Nos três modelos o consentimento é tido em alta conta, sendo utilizado como condição para a coleta e para o tratamento de dados. Sem exceção, vê-se o consentimento como fator legitimante da utilização dos dados pessoais, talvez como consequência da ideia de que, seja por uma ótica de direitos da personalidade ou por uma ótica econômica, a vontade do indivíduo é necessária para tornar sua disposição um ato justificado. Pela ótica econômica o consentimento é a via pela qual, geralmente, o titular dos dados cede seus dados a fim de obter um benefício (como é o caso de plataformas como Google e Facebook) e

aprova os termos pelos quais seus dados serão tratados, com clara remissão à liberdade contratual. Pela ótica dos direitos da personalidade, o interesse do indivíduo em um determinado benefício que lhe permita desenvolver sua própria personalidade é o fator legitimante da disposição de um direito que, normalmente, seria indisponível[47].

O segundo ponto em comum diz respeito à obrigação de transparência dos responsáveis pelo tratamento de dados pessoais, ou a um direito reflexo a obter informações sobre o tratamento. Apesar de haver ligeiras diferenças nos três modelos, todos preveem a necessidade de fornecer ao titular dos dados algumas informações básicas, antes do início do tratamento de dados. Mesmo nos Estados Unidos, onde não há uma norma específica para proteção de dados, a maioria das normas setoriais e também as normas de proteção ao consumidor[48] trazem obrigações sobre as informações a serem repassadas ao titular dos dados, logo no primeiro contato, as chamadas *privacy notices*.

Em terceiro, todos os modelos avaliados garantem alguns direitos básicos ao titular dos dados, entre eles o de acesso aos dados em tratamento e o de retificação ou eliminação, a depender do ato cabível. Com especial menção do modelo europeu, o direito de acesso é de suma importância para sua estratégia regulatória, vez que parte significativa da tutela reside na fiscalização pelo próprio titular dos dados. O direito de acesso consiste, talvez, no instrumento mais relevante de tais sistemas, pois permite o exercício dos demais direitos como de retificação, oposição, eliminação e contestação de decisões automatizadas - um assunto que adquire cada vez mais importância com os avanços em contratos eletrônicos e inteligência artificial.

O último ponto comum digno de nota diz respeito à segurança e ao sigilo dos dados pessoais. Os três países estudados exigem tanto medidas técnicas quanto físicas e administrativas ou organizativas para resguardar os dados pessoais. Apesar de isso parecer indicar simplesmente que há um reconhecimento geral à proteção dos dados pessoais, nem

---

[47] Há alguma discussão na literatura sobre a (in)disponibilidade da privacidade, principalmente quando enquadrada como direito da personalidade. No Brasil, especificamente, esse seria um direito indisponível, segundo o texto frio da lei. Obviamente, a interpretação evoluiu para acomodar a grande disparidade entre o que parece ser uma proibição absoluta e a prática comum. Confira-se: "Em uma série de situações não previstas em lei, mas socialmente admitidas, as pessoas desejam e aceitam limitar, pontualmente, o exercício de algum atributo da própria personalidade. O escritor que concede uma entrevista, revelando ao público detalhes da sua vida particular, deixa de exercer, naquela situação específica, seu direito à privacidade. Tal limitação, derivada da vontade do titular, não deve a toda evidência ser reprimida pela ordem jurídica, porque a vontade individual aí não se opõe, mas se dirige à realização da dignidade humana daquele indivíduo" SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. São Paulo: Atlas, 2013, p. 27.

[48] Como *Gramm-Leach-Bliley Act* (1999), *Fair Credit Reporting Act* (1970), e *Fair and Accurate Credit Transactions Act* (2003).

essa afirmação é verdade nem esse é o real significado desse fato. Os Estados Unidos, por exemplo, reconhecem um direito geral à privacidade com base em estatutos diversos, sendo os mais comuns o direito de propriedade e a responsabilidade civil: ora se protege o dado como um bem alienado ou cedido, outra com base na responsabilidade daquele que causa dano ao titular dos dados, seja por tratar indevidamente seus dados, seja por descuidar da segurança dos mesmos[49].

O que esse ponto comum vem indicar é que se o titular dos dados opta por fornecer certos dados pessoais por meio de um contrato, é responsabilidade de quem os recebe cuidar para que a expectativa do contratante – do consumidor, na maioria dos casos – seja cumprida, qual seja, de que apenas aquelas pessoas autorizadas, e para os fins autorizados, possam acessar e utilizar tais dados. No modelo uruguaio e no modelo europeu, tal conexão é mais simples, pois baseia-se antes no direito geral à proteção de dados, mas não deixa de ser também um argumento para exigir-se que os dados estejam seguros e sejam mantidos em sigilo.

b. Contrastes fundamentais

Buscar diferenças nos modelos mencionados, de uma maneira simples, é uma tarefa fácil, ainda que exija muito trabalho. No entanto, não buscamos aqui as pequenas diferenças, mas sim aqueles contrastes fundamentais em como cada modelo busca tornar efetivos os direitos e obrigações postos. Para melhor entender os contrastes entre os três modelos, buscamos enquadrá-los em três facetas da estratégia regulatória: o papel do Estado, o papel do mercado e o papel da tecnologia.

No quesito papel do Estado incluímos não só seu papel normativo, mas também fiscalizatório com a atuação das Autoridades de Proteção de Dados e órgãos semelhantes, e jurisdicional, com a atuação do Poder Judiciário. Os três modelos utilizam-se, de alguma forma, desses poderes para tutelar a proteção de dados, mas o fazem de modo diferente.

O modelo norte-americano, por seu lado, utiliza-se de normas setoriais para criar princípios e regras sobre proteção de dados em determinados contextos, mas não possui uma normativa forte e centralizadora, genérica, para garantir um direito geral à proteção de dados.

[49] "Consumers often bring class action lawsuits against organisations as a result of alleged privacy violations, such as statutory violations or other wrongful acts that affect them, such as information security breaches. In security breach cases, consumers often allege that the organisation was negligent in securing the consumers' personal information, and that such negligence led to the security breach." SOTTO, L.J.; SIMPSON, A.P. United States In: **Data Protection & Privacy 2015**, Londres: Law Business Research, 2015, pp. 213..

Há alguma atuação das autoridades fiscalizatórias, em geral também setoriais, mas têm ênfase em seu papel fiscalizador/sancionatório e normativo. De modo geral, o papel do Estado no modelo estadunidense é reduzido, e mesmo a legislação existente sobre o tema remete muitos assuntos à auto regulação. O Poder Judiciário aparece como recurso final para a resolução dos conflitos eventualmente surgidos durante a relação entre titular de dados e responsável pelo tratamento, mas tem grande importância para o modelo, dada a ausência de alternativas mais especializadas para a resolução de controvérsias.

O modelo uruguaio tem uma abordagem diferente, na medida em que possui normas centrais, abrangentes e generalistas, sobre proteção de dados, que reúnem os princípios básicos que devem informar as demais regras do sistema, qualquer que seja sua natureza. Mesmo os códigos de auto regulação são homologados com sua inserção no campo legislativo estatal, por normativa da respectiva Autoridade de Proteção de Dados. Talvez o ponto de maior interesse aqui seja o modelo fiscalizatório, baseado sobretudo no cadastramento prévio de bancos de dados, a cargo da Autoridade de Proteção, um caso singular na nossa análise. Na ausência de competência específica para solucionar contendas entre titulares e responsáveis pelo tratamento de dados[50], resta ao Judiciário solucionar casos relativos à proteção de dados pessoais. Um aspecto interessante do modelo é o remédio de Habeas Data, que foi adaptado e expandido, de modo a servir como ferramenta universal para execução específica de certas obrigações.

O modelo europeu, por seu lado, apesar de ter um grande número de normas centrais sobre proteção de dados pessoais, delega grande parte da competência legislativa – no que toca os aspectos técnicos e outros assuntos de grande especificidade – à Autoridade de Proteção de Dados. A recente reforma legislativa concedeu à Autoridade de Proteção ainda mais e maiores poderes fiscalizatórios e sancionatórios, permitindo a ela maior espaço de manobra. É de imenso interesse o papel central das Autoridades de Proteção no modelo europeu pois, além de suas competências normais, atuam também na resolução de conflitos diretamente entre as partes, em uma esfera administrativa, evitando-se assim a judicialização de inúmeros conflitos.

No que toca o papel do mercado, o modelo estadunidense talvez seja o que mais nele se fia, uma vez que sua regulação esparsa exige que grande parte da prática comum e

[50] Lembrando que a APD uruguaia pode, diante da denúncia do descumprimento de um direito de acesso, por exemplo, aplicar uma sanção (advertência, multa ou suspensão do banco de dados), mas não tem meios específicos para exigir o cumprimento da obrigação para com o titular dos dados.

aceitável seja definida pelos próprios agentes econômicos, seja por meio da prática contratual (sujeita a eventual inspeção judicial), seja pela autorregulação. Em um modelo onde a liberdade contratual é um dos fundamentos básicos da matéria, é de se esperar que a garantia de direitos venha através de incentivos econômicos para isso. Assim, ainda que não sempre no interesse do consumidor ou do titular dos dados, há abertura para que a privacidade do consumidor seja definida pelo retorno esperado. Como dissemos ao início do texto, com a crescente conscientização, exige-se cada vez mais dos provedores de serviço, que devem se adequar para não perder relevância competitiva.

O modelo uruguaio é, dentre os modelos analisados, o que menos recorre ao mercado para tentar moldar comportamentos. O modelo de tutela impositivo, como descrito anteriormente, ignora parcialmente o valor dos mecanismos econômicos e seu impacto regulatório, fazendo mera referência a códigos de conduta, sem outros pontos de contato interessantes entre Direito e Economia.

O modelo europeu, apesar de não trazer a definição exata da coleta e do tratamento de dados na lei, apresenta-nos uma abordagem interessante para o papel do mercado em um modelo regulatório. Em suma, a União Europeia utiliza mecanismos de mercado para incentivar a adesão a padrões de tutela já definidos nas normas sobre proteção de dados. Tais mecanismos geralmente funcionam em uma base de troca, sendo que os agentes que optarem por aderir a tais regras podem receber benefícios competitivos por isso. O exemplo mais óbvio dessa política é justamente o sistema de certificação criado pelo GDPR, que permite às empresas utilizarem certos certificados e selos de qualidade quando seja constatado o cumprimento substancial das normas em vigor. No contexto atual, em que a privacidade ganha importância para o cidadão comum, a vantagem competitiva oferecida acaba por criar interesses convergentes das duas pontas da transação: proteger a privacidade do usuário deixará de ser um custo para se tornar um diferencial competitivo e uma fonte de receitas.

Por fim, a tecnologia em si tem um papel nos modelos regulatórios. Enquanto todos recomendam certas medidas de segurança e sigilo (como a adoção da criptografia e do processo de anonimização), o modelo europeu possui um diferencial de nota na matéria. Com especial reforço na recente reforma legislativa, os conceitos de *privacy by design and by defaut* e *privacy enhancing technologies*, ganham espaço e incentivam alterações na "arquitetura normal" - o modo e o que a tecnologia permite em razão do modo como é construída - para fazer com que o próprio valor da privacidade tenha lugar na concepção

inicial de qualquer serviço ou produto. Essa característica, no entanto, é arriscada na medida em que, incorporada na GDPR, diminui a neutralidade tecnológica do texto e arrisca torná-lo obsoleto mais cedo do que seria esperado.

c. Modelos regulatórios

Com base nas observações anteriores, ousamos propor o conceito de três estratégias ou modelos regulatórios para a proteção de dados pessoais: o modelo normativo-estatal, o modelo liberal, e o modelo eclético.

O modelo normativo-estatal tem como exemplo, neste trabalho, o Uruguai. Suas principais características seriam um sistema normativo centralizador, mantendo a maior parte das competências regulatórias e fiscalizatórias no próprio Estado, através da forte atuação do Poder Judiciário, onde um procedimento processual específico é utilizado para possibilitar o exercício de direitos.

O modelo liberal, obviamente, inspira-se no modelo dos Estados Unidos, onde há grande recurso à autorregulação e onde o estado busca interferir, criando normas, apenas em áreas consideradas sensíveis, como saúde, finanças e menores de idade. Nesse modelo, apesar de haver alguma tendência à judicialização, o principal foco é a liberdade de contratação e a possibilidade de o mercado definir, em sua interação com os consumidores, os comportamentos aceitáveis.

O último modelo tem como exemplo a União Europeia e sua abordagem à proteção dos dados pessoais. O modelo eclético é assim nomeado pois resulta de um grande ajuntamento de estratégias, incluindo o recurso a normas estatais e mercadológicas, mecanismos alternativos de resolução de controvérsias, soluções tecnológicas e o engajamento ativo, tanto do titular dos dados quanto do responsável pelo tratamento de dados, no cumprimento e fiscalização da lei. Esse último ponto talvez seja o mais interessante, por trabalhar não pela repressão de condutas (onde cumprir a lei é um modo de não perder dinheiro), mas pela indução, onde o respeito à privacidade é interessante para todos os envolvidos, pelos benefícios daí advindos.