UNIVERSIDADE DE SÃO PAULO
CENTRO DE ESTUDOS SOCIEDADE E TECNOLOGIA

Facilitando *the Cloud*:
A Regulamentação da Proteção de Dados como um Impulsor da Competitividade Nacional na América Latina

Horacio Gutiérrez e Daniel Korn
Maio 2014

Facilitando *the Cloud*: A Regulamentação da Proteção de Dados como um Impulsor da Competitividade Nacional na América Latina

Horacio E. Gutiérrez[1] e Daniel Korn[2]

Os investimentos em infraestrutura de Internet em toda a América Latina estão começando a gerar retorno, particularmente à medida que consumidores,

1. Vice-Presidente Corporativo e Conselheiro Geral Adjunto, Microsoft Corporation. O Sr. Gutiérrez foi nomeado o "Advogado das Américas de 2013" pela revista publicada pela School of Law da Universidade de Miami, *Inter-American Law Review*. Este artigo foi originalmente publicado pela Universidade de Miami *Inter-American Law Review* como "*Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America*" (Volume 45, Number 1 (2013)).

2. Diretor de Assuntos Corporativos, Microsoft América Latina.

empresas, agências governamentais, prestadores de serviços de saúde e instituições de ensino usam conexões de Internet para acessar serviços inovadores de computação em nuvem.[3] De fato, o mercado de computação em nuvem na América Latina deverá crescer a uma taxa anual de 70 por cento entre 2012 e 2016.[4] Isto não surpreende, uma vez que a computação em nuvem proporciona aos usuários com conexão à Internet, um meio acessível em um nível de poder na computação que, até recentemente, estava disponível somente para as empresas que dispusessem de grandes orçamentos de TI e profissionais capacitados.[5] Ademais, essa tecnologia tem um enorme potencial para criar novos empregos, reduzir os custos e promover a inclusão social.[6]

Não obstante as considerações anteriores, a adoção da computação em nuvem na América Latina ainda está em seu estágio inicial, e as decisões tomadas hoje pelos formuladores de políticas e outros envolvidos influenciarão o quanto essa tecnologia poderá beneficiar os cidadãos de determinados países, e da região como um todo, a curto e médio prazo. As regras e políticas do século XXI para proteção de dados, e o fato de serem projetadas com a flexibilidade necessária para acomodar esta tecnologia inovadora, desempenharão um papel importante para facilitar a adoção da computação em nuvem e nos benefícios que ela pode gerar para a *competitividade nacional*, ou seja, o crescimento econômico e melhoria a longo prazo do padrão de vida em decorrência do aumento da produtividade e eficiência no país.[7] Os formuladores de políticas de toda a região devem evitar o caminho fácil e estarem prontos para tomar decisões políticas muitas vezes difíceis, porém necessárias para o desenvolvimento de regras de proteção de dados que permitirão que seus países assumam a liderança nessa nova era de computação em nuvem para beneficiar os seus cidadãos.

---

3. "Computação em nuvem" pode ser definido como um modelo para acesso à rede, de forma conveniente e sob demanda, para usar recursos de computação que estão em um *pool* compartilhado e podem ser rapidamente fornecidos por meio de um esforço mínimo de gerenciamento ou interação com o provedor de serviços. *Ver a definição de Computação em Nuvem da NIST*, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

4. *Ver "O mercado de computação em nuvem na América Latina vale 280 milhões de dólares em 2012, segundo a IDC"*, Start Up in Brazil (4 de setembro de 2012), http://startupbrazil.co.uk/latin-american-cloud-computing-worth-us280mn-2012-idc/.

5. *Ver* Alexa Huth e James Cebula, *The Basics of Cloud Computing*, U.S. Computer Emergency Readiness Team, *disponível em* http://www.us-cert.gov/sites/default/files/publications/CloudComputingHuthCebula.pdf (explica como computação em nuvem é um recurso que pode ser facilmente acessado por indivíduos e empresas).

6. *Ver Cloud Will Generate 14 Million Jobs by 2015: That's a Good Start*, Joe McKendrick, Forbes (5 de março de 2012, 8:21 PM), http://www.forbes.com/sites/joemckend rick/2012/03/05/cloud-will-generate-14-million-jobs-by-2015-thats-a-good-start/.

7. Orlando Ayala, *Defining National Competitiveness*, Future Gov (20 de maio de 2011), http://www.futuregov.asia/articles/2011/may/20/defining-national-competitiveness.

Este artigo examina como os governos e a indústria da região podem conquistar a confiança do consumidor na nuvem por meio de regras equilibradas e consistentes de proteção de dados, com o intuito de aumentar a competitividade nacional. A Parte I analisa como as regras de privacidade de dados podem potencializar o uso da computação em nuvem. A Parte II explora os enormes benefícios que a computação em nuvem oferece para a competitividade nacional.

A Parte III destaca os desafios regulatórios impostos pela computação em nuvem, incluindo a experiência inicial da regulamentação da nuvem e o papel que a indústria desempenha no estabelecimento da confiança do cliente na nuvem, encerrando especificamente com uma descrição da abordagem da Microsoft sobre estas questões.

I. A COMPUTAÇÃO EM NUVEM ESTÁ AUMENTANDO A IMPORTÂNCIA DAS REGRAS EQUILIBRADAS DE PRIVACIDADE DE DADOS

A preocupação com a privacidade já existia muito antes do advento da nuvem, da Internet, ou até mesmo dos computadores. Há séculos, as pessoas têm procurado controlar o uso e a divulgação de seus dados pessoais.[8] Hoje, muitos governos no mundo inteiro estão avaliando a necessidade de leis para acompanhar as novas exigências e realidades da computação em nuvem e, ao mesmo tempo, obter os mesmos benefícios que há tanto tempo têm impulsionado a legislação de privacidade: potencializar as decisões individuais relativas à privacidade, mantendo a segurança da informação e desenvolver a confiança em um grande avanço na tecnologia, que promete transformar a sociedade de forma positiva, se administrado corretamente. Na Europa, a representante oficial da Agenda Digital, Neelie Kroes, pediu a adoção de regras "claras e amigáveis para a nuvem... [porque] uma "nuvem" sem proteção de dados forte e transparente não é o tipo de nuvem de que precisamos."[9] Do mesmo modo, o Departamento de Comércio dos EUA observou recentemente que a capacidade de "aproveitar de forma segura todo o potencial de serviços, como e-mail e armazenamento de arquivos baseado em nuvem, depende de proteções de privacidade que sejam consistentes com outros modelos de computação."[10] Nós estamos de acordo.

8. *Ver, por exemplo*, Robert Ellis Smith, Ben Franklin's Website: Privacy and Curiosity from Plymouth Rock to the Internet, (Privacy Journal, 2004) (discute o desejo dos americanos por privacidade durante toda a história dos Estados Unidos).

9. Neelie Kroes, Vice-Presidente da Agenda Digital, Com. Europeia, Discurso na Conferência Les Assises du Numérique: *Cloud Computing and Data Protection* (25 de novembro de 2010), *disponível em* http://europa.eu/rapid/press-release_SPEECH-10-686_en.htm.

10. *Ver* Força-tarefa da Internet do Departamento de Comércio dos EUA, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dezembro de 2010), *disponível em* http://www.commerce.gov/sites/default/files/documents/2010/de cember/iptf-privacy-green-paper.pdf.

Em poucas palavras, é de interesse coletivo que todos os usuários da nuvem tenham uma confiança solidamente estabelecida na nuvem.

Na América Latina, o interesse na proteção de dados também está em ascensão.[11] Desde a década de 80, muitos governos da região passaram a oferecer aos cidadãos o direito constitucional de acesso e retificação de seus dados pessoais. Também conhecida como "habeas data", essa proteção visa "salvaguardar a liberdade individual contra abusos na era da informação."[12] Um Habeas garante "um controle real sobre os dados pessoais confidenciais, impedindo o abuso de tais informações, o que seria prejudicial para o indivíduo."[13] Como essas disposições do habeas data normalmente formam parte das constituicões nacionais, recebem "do mais alto nível de proteção possível, e de procedimentos mais céleres nos melhores tribunais."[14] Por exemplo, a Seção 43(3) da Constituição da Argentina prevê um forte direito ao habeas data:

> Qualquer pessoa poderá interpor esta ação para tomar conhecimento dos dados a ela referentes e da sua finalidade, que constem em registros ou bancos de dados públicos, ou em registros ou bancos de dados privados destinados a fornecer informações, e em casos de falsidade ou discriminação, para a supressão, retificação, confidencialidade ou atualização dos mesmos. A natureza secreta das fontes de informação jornalística não deve ser prejudicada.[15]

A partir de 2000, os países da América Latina passaram a aprovar leis abrangentes de proteção de dados, que são baseadas na Diretiva de Proteção de Dados da Europa de 1995.[16] Estas leis variam amplamente, porém tais leis geralmente contêm restrições "pré-nuvem" sobre o uso e a transferência de dados, exigem o consentimento expresso do titular dos dados antes do processamento,

11. *Ver* Aldo M. Leiva, *Data Protection Law in Spain and Latin America: Survey of Legal Approaches*, 41 Int'l Law News 4 (2012), *disponível em* http://www.americanbar.org/publications/international_law_news/2012/fall/data_protection_law_spain_latin_ america_survey_legal_approaches.html.

12. Enrique Falcón, H´abeas Data: Concepto y Procedimiento 28 (1996).

13. Andrés Guadamuz, *Habeas Data vs. the European Data Protection Directive*, 3 J. Int'l T.5 (2001).

14. *Id.*

15. Art. 2, Constitución Nacional (Arg.), *tradução do autor*.

16. Leiva, *supra* nota 11 ("abordagens espanholas e latino-americanas para a proteção de dados pessoais estão enraizadas no conceito europeu de direitos de privacidade pessoal que se desenvolveram por toda a Europa durante várias décadas e culminaram, via integração regional, na adoção da Diretiva de Proteção de Dados Europeia («Diretiva») em 1995.").

permitem que indivíduos acessem e corrijam cada iteração possível dos seus dados pessoais, além de exigirem medidas de proteção para segurança dos dados.

Em 2000, a Argentina promulgou a primeira lei abrangente de proteção de dados da região, que continha muitos dos elementos da diretiva pré-nuvem da União Europeia de 1995.[17] O Uruguai adotou uma lei similar de proteção de dados anos mais tarde.[18] Começando com a adoção da lei do México que marcou um precedente em 2010, a consideração, e muitas vezes a adoção, de leis abrangentes de proteção de dados tornou-se a norma na América Latina, como mostra a tabela[19] abaixo.

País	**Pontos principais**
Argentina	1. A Argentina adotou uma lei similar a da UE em 2000 e recebeu uma determinação de adequação da CE em 2003. 2. De forma geral, transferências internacionais de dados da Argentina estão proibidas, a menos que os proprietários dos dados concedam autorização prévia e expressa, caso o país de destino não tenha leis que o legislador argentino considere ser "adequadas". Nenhum "porto seguro" foi criado para facilitar a transferência de dados para países que não forem considerados "adequados".
Brasil	1. O Brasil não tem uma lei abrangente de proteção de dados, embora, como em muitos países da região, exista um direito constitucional à privacidade, de forma geral. O Ministério da Justiça elaborou um projeto de lei e o colocou em discussão pública em 2011. Mais recentemente, o Congresso Nacional começou a considerar um projeto de lei que permitiria que o presidente exigisse que dados pessoais dos cidadãos brasileiros fossem mantidos no país.
Chile	1. O Chile adotou uma lei de proteção de dados em 1999, mas ela não é considerada de natureza "abrangente". 2. Em janeiro de 2012, o Poder Executivo apresentou ao Congresso chileno uma proposta de Projeto de Lei com o objetivo de criar uma lei abrangente de proteção de dados. Em novembro de 2013, o Projeto de Lei ainda estava sendo analisado por uma comissão do Congresso.
Colômbia	1. A Colômbia aprovou uma lei abrangente de privacidade de dados, com ação final tomada em outubro de 2012, quando a Lei 1.581 foi promulgada. 2. Similar às leis da Argentina e do Uruguai, a nova lei proíbe a transferência internacional de dados para os países que não tiverem regimes "adequados" de proteção de dados, conforme determinação do órgão regulador colombiano, a menos que os proprietários dos dados concedam autorização prévia e expressa. O Decreto 1377 foi publicado em junho de 2013.
Costa Rica	1. A Costa Rica aprovou uma lei abrangente de privacidade de dados em setembro de 2011. Entre outros requisitos, dados pessoais, em geral, não podem ser processados sem o consentimento expresso da pessoa em questão. 2. Em março de 2013, do Ministério da Justiça e da Paz publicou regulamentos sob a nova lei. De forma absolutamente singular, os regulamentos exigiriam que controladores de dados fornecessem à autoridade de proteção de dados uma "super conta de usuário" com acesso total e irrestrito. 3. Uma circular presidencial publicada em 15 de maio de 2013 promove especificamente a compra em nuvem no setor público.

17. Lei No. 25326, 30 de outubro de 2000, (Arg.).

18. L. 18.331, 11 de agosto de 2008, DIÁRIO OFICIAL (Urug.).

19. Esta tabela foi preparada por Matt DelNero, da Covington & Burling LLP, em 8 de novembro de 2013.

República Dominicana	1. Em 22 de abril de 2013, o Senado da República Dominicana aprovou uma lei de Proteção de Dados suplementar ao artigo 44.2 da Constituição da República Dominicana. O projeto de lei aguarda votação na Câmara dos Deputados. 2. O projeto de lei segue muitos dos princípios e conceitos encontrados na Diretiva de Proteção de Dados da UE, tais como limitações sobre a transferência de dados, proteção especial para dados confidenciais e a criação de uma autoridade independente de proteção de dados. O projeto também requer o consentimento dos pais para o processamento de dados sobre crianças menores de 16 anos de idade.
México	1. O México adotou uma legislação de privacidade de dados em 2010. Regulamentos dos termos da lei foram publicados em dezembro de 2011. 2. A lei mexicana pode fornecer uma "terceira via" entre a abordagem ad hoc que prevalece nos Estados Unidos e a abordagem mais prescritiva adotada na Europa e, cada vez mais, em muitos países da América Latina. Por exemplo, a lei prevê maior flexibilidade na transferência de dados internacionais. Além disso, embora adote o princípio do consentimento, a lei deixa claro que, em muitos casos, esse consentimento pode ser obtido tacitamente por meio de divulgações apropriadas em um aviso de privacidade. 3. O México adotou os princípios de proteção de dados estabelecidos pelo Fórum de Cooperação Econômica Ásia-Pacífico (APEC), em vez da abordagem mais restritiva da Diretiva de Proteção de Dados da UE. Além de elementos da APEC contidos na lei, a partir de janeiro de 2013 o México tornou-se o segundo signatário formal (após os EUA) das Regras de Privacidade Transnacional da APEC. 4. Novas diretrizes para avisos de privacidade entraram em vigor em 17 de abril de 2013. De maneira similar às regras da UE, as novas diretrizes exigem que controladores forneçam os avisos com a devida antecedência e obtenham o consentimento do proprietário dos dados pessoais antes que eles sejam coletados por meio de cookies, web beacons ou outros meios automatizados.
Nicarágua	1. A Nicarágua aprovou uma lei abrangente de proteção de dados em Março de 2012. 2. Em geral, a nova lei segue um modelo baseado nas diretivas da UE. Ela também inclui conceitos como o "direito a ser esquecido", que refere-se a um direito de ter todos os vestígios de seus dados apagados dos registros de uma empresa.
Peru	1. A Lei de proteção de dados do Peru de 2011 também segue o modelo da UE, mas com meios um pouco mais modernos de permitir fluxos de dados considerados cruciais para a computação em nuvem. Especificamente, apesar de a regra padrão exigir o consentimento para transferência de dados para países sem leis "adequadas" de proteção de dados, o controlador pode superar esse obstáculo se tomar medidas para tornar-se responsável pela proteção dos dados quando esses forem transferidos para fora do país. 2. O Peru aprovou por decreto regulamentos nos termos da lei, em 22 de março de 2013. O regulamento contém uma disposição sobre computação em nuvem ("*tratamiento de datos personales por medios tecnológicos tercerizados*", expressão que pretende ser uma descrição tecnologicamente neutra, permitindo desenvolvimentos tecnológicos ainda desconhecidos no futuro). A provisão permite que os controladores utilizem serviços em nuvem de terceiros, desde que garantam que o provedor da nuvem está em conformidade com os requisitos de proteção de dados previstos na lei. Além disso, o próprio prestador de serviços na nuvem deve ser responsabilizado nos termos do contrato com o controlador.
Uruguai	1. O Uruguai adotou uma lei similar à diretiva da UE em 2008 e recebeu uma determinação de adequação da CE em 21 de agosto de 2012. 2. Transferências internacionais de dados do Uruguai são proibidas caso o país de destino não tenha leis "adequadas". No entanto, ao contrário da vizinha Argentina, a DPA uruguaia emitiu uma resolução reconhecendo como "adequado" qualquer país de destino assim reconhecido pela UE. Entendemos que esta resolução tem sido interpretada para permitir a transferência para qualquer organização certificada como porto seguro pelos EUA e pela UE.

II. O ESTÍMULO A MAIOR COMPETITIVIDADE NACIONAL REQUER UMA POLÍTICA REGULATÓRIA EQUILIBRADA DE PROTEÇÃO DE DADOS PARA COMPUTAÇÃO EM NUVEM

A nuvem fornece recursos de computação em *pool*, que estão disponíveis sob demanda a qualquer momento, a partir de qualquer dispositivo conectado à Internet.[20] Prestadores de serviços em nuvem operam uma rede global de *data centers* para prestar um serviço contínuo para uma base de clientes espalhada por todo o mundo.[21] Esta seção descreve os principais benefícios econômicos da computação em nuvem e os elementos de uma política regulamentar equilibrada, que poderia ajudar a promover a adoção pelo consumidor e o crescimento desta tecnologia notável em benefício da comunidade.

A. Benefícios da Nuvem

Poucas tecnologias recentes têm apresentado mais benefícios econômicos potenciais do que a nuvem. Espera-se que, para 2014, o mercado mundial de computação em nuvem equivalerá a US$150 bilhões.[22] Especialmente em mercados emergentes, a computação em nuvem pode se tornar um impulsor do crescimento econômico e de índices sociais.[23] A nuvem oferece aos países desenvolvidos e em desenvolvimento uma ampla gama de benefícios. Cada benefício descrito a seguir deve ser de particular interesse para as empresas de pequeno e médio porte (PME), que empregam cerca de 67 por cento da força de trabalho na América Latina e, em muitos casos, não têm sido capazes de alavancar o poder de computação de forma significativa até o presente.[24]

1. Criação de Empregos Através da Inovação

A computação em nuvem tem o potencial de gerar empregos através da inovação local. Isso ocorre, em grande parte, porque a computação em nuvem está diminuindo os custos de manutenção contínua de infraestrutura e aplicativos legados, bem como a necessidade de grandes investimentos em tecnologia, permitindo, portanto, que as empresas apliquem seus orçamentos em *novos mercados* e *novos produtos*, que, por sua vez, geram crescimento do número de empregos.[25]

---

20. *Ver* Huth, *supra* nota 5.

21. *Id.*

22. Andrew R. Hickey, *Cloud Computing Services Market To Near $150 Billion in 2014*, CRN (22 de junho de 2010, 12:46 PM), http://www.crn.com/news/managed-services/225700984/cloud-computing-services-market-to-near-150-billion-in-2014.htm.

23. *Ver With Cloud, SMBs Will Lead Emerging Economies Across the Digital Divide*, Cisco (Setembro de 2012), http://www.cisco.com/web/about/ac79/docs/FastFacts/Fast Facts_Cloud-and-Digital-Divide.pdf.

24. Angel Gurría, *Latin American Economic Outlook 2013: SME Policies for Structural Change* (OECD 2012), *disponível em* http://www.keepeek.com/Digital-Asset-Management/oecd/development/latin-american-economic-outlook-2013_leo-2013-en.

25. *Ver, por exemplo*, Mohana Ravindranath, *Analysts expect growth in cloud jobs*, Wash. Post (15 de agosto de 2013, 8:00 AM), http://www.washingtonpost.com/business/on-it/ana lysts-expect-growth-in-cloud-jobs/2013/08/14/56d5715a-04fb-11e3-a07f-49ddc7417125 _story.html ("Em diversos setores, a economia de custos associada à mudança para a um modelo de computação em nuvem não significou um aumento do desemprego, mas sim dos recursos disponíveis para investimento em outros aspectos do negócio. . .").

De fato, no que diz respeito ao setor de Tecnologia da Informação, em particular, os especialistas acreditam que a computação em nuvem será o motor do aumento do índice de emprego na próxima década. De acordo com um *white paper* da IDC publicado em novembro de 2012 e patrocinado pela Microsoft, a demanda mundial por empregos relacionados à nuvem crescerá 26 por cento ao ano até 2015, criando até 7 milhões de empregos relacionados à nuvem no mundo inteiro.[26] Até 2015, o número de empregos relacionados à nuvem crescerá a uma taxa anual de 22 por cento na América do Norte e 24 por cento na Europa, enquanto mercados emergentes da América Latina, Europa Central e Oriental, Oriente Médio e Ásia-Pacífico terão a maior taxa de crescimento do emprego vinculada à nuvem: 34 por cento anualmente.[27]

Milhões desses novos postos de trabalho são altamente qualificados e oferecem os altos salários que os governos estão ansiosos para atrair. Por exemplo, em um estudo publicado pela Comissão Econômica para a América Latina e Caribe (CEPAL), a análise feita pelos economistas Andrea Colciago e Federico Etro concluiu que a adoção da computação em nuvem por empresas no Brasil pode resultar na criação de 900 mil novos postos de trabalho.[28] Da mesma forma, o Instituto Mexicano para a Competitividade (IMCO) descobriu recentemente que a tecnologia em nuvem no México pode criar 1.800 novas pequenas e médias empresas, que, somadas, empregariam cerca de 63.400 empregados. Esses dados são baseados em uma estimativa conservadora da economia, gerada pela redução de apenas um por cento dos custos fixos das empresas em decorrência dos benefícios da nuvem.[29]

2. Redução de Custos

Além da criação de empregos altamente qualificados, a computação em nuvem impulsiona a economia, proporcionando às empresas e agências governamentais redução significativa nos custos dos serviços e infraestrutura de TI.[30]

---

26. Cushing Anderson e John F. Gantz*, Climate Change: Cloud's Impact on IT Organizations and Staffing*, IDC 1, 3 (Novembro de 2012), http://www.microsoft.com/en-us/ news/download/presskits/learning/docs/idc.pdf.

27. *Id.* em 4-5.

28. *Ver* Valeria Jordán et al., *Banda Ancha en América Latina: Más allá de la Conectividad*, CEPAL 1, 29 (Fevereiro de 2013), http://www.cepal.org/publicaciones/xml/2/ 49262/BandaAnchaenAL.pdf.pdf.

29. "*Computo en la Nube": Nuevo Detonador para la Competitividad de M´exico*, Instituto Mexicano para a Competitividade A.C. (IMCO), "Computo en la Nube": Nuevo detonador para la competitividad de México, em) 1, 31 (Maio de 2012), http://imco.org.mx/images/pdf/Computo_en_la_Nube-detonador_de_competitividad_doc.pdf [a partir de agora chamado de *Relatório sobre Nuvem do IMCO*].

30. *Ver* Hilary Kramer, *Washington Moves Into the Cloud: Saving Money and Securing Data*, Forbes (8 de julho de 2013, 6:45 AM), http://www.forbes.com/sites/hilarykra mer/2013/07/08/washington-moves-into-the-cloud-saving--money-and-securing-data/.

Dados recentes sugerem que a implantação de uma nuvem híbrida reduziria a despesa total de TI em cerca de 20 a 30 por cento.[31] Como qualquer empresa ou organização pode se conectar a todos os benefícios da nuvem com uma simples conexão da Internet, não existe a necessidade de investimentos iniciais. Gerações anteriores de tecnologia exigiam investimentos significativos em servidores e outros equipamentos físicos, mas esse capital é desnecessário com a computação em nuvem. Ao agregar a demanda por computação, a nuvem permite um aumento nas taxas de utilização dos servidores. O IMCO estima que o setor público no México pode economizar 1,7 por cento de seus gastos anuais migrando para a nuvem.[32] É importante destacar que essas economias de custo servem para aumentar a democratização da computação, gerando maior inclusão social, como será discutido na próxima seção.

Além disso, os *data centers* de grande escala resultam em menores custos por servidor porque exigem menos energia para operação.[33] À medida que aumenta o número de clientes, diminui o custo de servidor por inquilino e de gerenciamento de aplicativos. Em uma empresa tradicional, sem nuvem, um único administrador de sistemas pode atender aproximadamente 140 servidores.[34] Em contraste, uma central de nuvem normalmente administra milhares de servidores simultaneamente, que são capazes de lidar com várias tarefas ao mesmo tempo.[35] Esta eficiência permite que os funcionários de TI se concentrem em atividades de maior valor agregado, como o desenvolvimento de novos recursos e atendimento às solicitações dos usuários.

A correspondente economia de energia também poderia se traduzir em uma redução de emissão de carbono, motivo pelo qual a computação em nuvem tem sido chamada de "TI verde".[36]

31. *Business Agility and the True Economics of Cloud Computing*, VMware 1, 6 (2011), https://www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_and_ the_True_Economics_of_Cloud_Computing_White_Paper.pdf.

32. Relatório sobre Nuvem do IMCO, *supra*nota 29, em 34.

33. *Ver, por exemplo*, Yuan Yao et al., *Data Centers Power Reduction: A Two Time Scale Approach or Delay Tolerant Workloads* (2012), http://www.eecs.berkeley.edu/~huang/ data-center-power-infocom12.pdf (discute como os grandes *data centers* têm o potencial de reduzir os custos de energia).

34. *Ver* Rich Miller, *How Many Servers Can One Admin Manage?*, *Data center* Knowledge (30 de dezembro de 2009), http://www.datacenterknowledge.com/archives/2009/12/ 30/how-many-servers-can-one-admin-manage/.

35. *Ver* Clair Cain Miller e Quentin Hardy, *Google Elbows Into the Cloud*, N.Y. Times (12 de março de 2013), http://www.nytimes.com/2013/03/13/technology/google-takes-on-amazon-and-microsoft-for-cloud-computing-services.html?pagewanted=all.

36. Relatório sobre Nuvem do IMCO, *supra*nota 29, em 40.

O IMCO estima que a migração para a nuvem de empresas de médio e grande porte no México, juntas gerariam uma redução das emissões de carbono equivalente à remoção de 90.000 carros de circulação.[37]

3. Democratização da Computação e Inclusão Social

A computação em nuvem não só aumenta a eficiência, como também aumenta a igualdade. Ao fornecer acesso a um nível de poder computacional antes disponível somente para grandes corporações e economias desenvolvidas, a nuvem é a próxima etapa na democratização da informática e no aumento da inclusão social.[38] Com a computação em nuvem, organizações de qualquer tamanho e em praticamente qualquer lugar do mundo podem aproveitar o poder da supercomputação e dos aplicativos de *software* que antes estavam disponíveis somente para as maiores empresas globais.[39] Indivíduos também podem usar a nuvem para desenvolver ferramentas de computação totalmente novas. Por exemplo, a nuvem permite que os funcionários em hospitais rurais consultem especialistas do mundo inteiro em tempo real, oferecendo aos moradores rurais cuidados médicos que eles jamais seriam capazes de receber antes do advento da computação em nuvem.[40] A nuvem também reduz os custos dos hospitais para o armazenamento de raios-x e outros arquivos volumosos de saúde.[41] De fato, o uso de computação em nuvem em hospitais deve crescer a uma taxa anual composta de 20,5 por cento entre 2012 e 2017.[42]

Da mesma forma, a nuvem tem apresentado oportunidades sem precedentes para os distritos escolares rurais e de baixa renda.[43] A nuvem fornece às escolas aplicativos poderosos baseados na *web*, ensino à distância e armazenamento de baixo custo.[44] Por meio da nuvem, escolas de pequeno porte podem ter acesso a materiais educacionais que jamais estariam disponíveis de outra forma. Além disso, a nuvem permite que governos dêem um salto gigante na prestação de serviços aos cidadãos.

---

37. Relatório sobre Nuvem do IMCO, *supra*nota 29, em 40.

38. Joe Mullich, *16 Ways the Cloud Will Change Our Lives*, WALL ST. J. (7 de janeiro de 2011), http://online.wsj.com/ad/article/cloudcomputing-changelives.

39. *Ver* Huth, *supra* nota 5.

40. Pam Belluck, *Nantucket Hospital Uses Telemedicine as Bridge*, N.Y. TIMES, (8 de outubro de 2012), http://www.nytimes.com/2012/10/09/health/nantucket-hospital-uses-telemedicine-as-bridge-to-mainland.html?pagewanted=all.

41. Ken Terry, *Cloud Computing in Healthcare: The Question Is Not If, But When*, FIERCEHEALTHIT (9 de janeiro de 2012), http://www.fiercehealthit.com/story/cloud-computing-healthcare-question-not-if-when/2012-01-09.

42. Bernie Monegain, *3 Big Trends for the EHR Cloud*, Healthcare IT News (8 de outubro de 2012), http://www.healthcareitnews.com/news/3-big-trends-ehr-cloud.

43. *Ver* KerriLee Horan, *Saved by the Cloud*, DISTRICT ADMINISTRATION (Fevereiro de 2010), http://www.districtadministration.com/article/saved-cloud.

44. Diane Weaver, *Six Advantages of Cloud Computing in Education*, PEARSON (Abril de 2013), http://www.pearsonschoolsystems.com/blog/?p=1507.

Por exemplo, com sede em Porto Rico, a Rock Solid desenvolveu um linha de assistência ao cidadão baseada em nuvem para o governo do Panamá. O serviço permite que os residentes do Panamá disquem 1-3-1 para acessar uma central que os conecta diretamente às agências governamentais.[45] Da mesma forma, o sistema de educação da Colômbia tem usado a nuvem para melhorar os testes padronizados de desempenho dos alunos.[46] Sem essa tecnologia, o Instituto Colombiano de Avaliação Educacional (ICFES) precisaria usar milhares de servidores próprios para disponibilizar esses resultados aos alunos duas vezes ao ano.[47] Com a computação em nuvem, o ICFES aproveitou a escala e a natureza sob demanda da nuvem, poupando seus servidores para atender essa necessidade. Essa solução beneficiou o governo, bem como os alunos, pais e professores.

O que mais nos empolga é o que a eficiência da computação em nuvem representa ao derrubar uma grande barreira que dividia nossas sociedades entre aqueles que *poderiam* fazer um alto investimento em capital inicial ou operacional para acessar e atualizar as mais recentes tecnologias de *software* que são cada vez mais necessárias para os negócios e aqueles que não poderiam fazer esse investimento. Como o acesso a computação em nuvem tem um preço inicial mais baixo, essa distinção infeliz tende a desaparecer, e a interação regular com o *software* mais recente deve se tornar uma realidade muito mais presente para a comunidade em geral.

4. Maior Agilidade

A computação em nuvem também permite que empresas e organizações governamentais se adaptem aos novos desafios e exigências com maior agilidade. A capacidade inédita de armazenamento e poder computacional disponível hoje na nuvem permite que as organizações implantem novos aplicativos e serviços com uma velocidade significativamente maior – e menor risco – do que no passado.[48] Serviços que costumavam exigir grandes investimentos de capital e implantações demoradas agora podem ser lançados em questão de semanas ou mesmo dias.

45. *Ver* o vídeo da Rock Solid Technologies, *Dynamics CRM & Rock Solid Republic of Panama-311 System*, YouTube (6 de abril de 2011), http://www.youtube.com/watch?v=HV UCALNG2D4.

46. Hernán Rincón, *This is Latin America's Decade: The Cloud Will Make it Possible*, Americas Quarterly (2º semestre de 2011), http://www.americasquarterly.org/node/ 3085.

47. *Id.*

48. *Ver, por exemplo*, Reuven Cohen, *Build Your Own Web or Mobile App In Minutes With These Cloud Based Tools*, Forbes (22 de março de 2013), http://www.forbes.com/sites/ reuvencohen/2013/03/22/build-your-own-web-or--mobile-app-in-minutes-with-these-cloud-based-tools/ (explica como a nuvem pode ser usada por empresas para criar aplicativos rapidamente).

No passado, quando as empresas passavam por surtos repentinos de popularidade, seus servidores *web* públicos e internos eram muitas vezes incapazes de lidar com o aumento da demanda. Quando um terremoto devastou a Costa Rica em 5 de setembro de 2012, tornando inoperáveis as comunicações tradicionais, tais como telefones, rádios e televisões, os moradores conseguiram obter informações visitando o site da rede de televisão nacional (Teletica), uma vez que o site estava hospedado na nuvem, e a capacidade de Internet do site pôde ser ampliada para atender ao aumento da demanda.[49] Com a computação em nuvem, as empresas puderam facilmente se adaptar ao aumento da demanda porque não estavam limitadas à capacidade de seus servidores internos. De acordo com um levantamento dos responsáveis pela tomada de decisões corporativas, realizado pela AbsolutData para a VMware em fevereiro de 2011, 65 por cento dos entrevistados acreditam que a nuvem tem um "papel fundamental" no aumento da agilidade e que a computação em nuvem "ajudaria suas organizações a manter uma arquitetura flexível para suportar mudanças."[50]

Essa flexibilidade é, em grande parte, decorrente da mobilidade da nuvem. Ela não só fornece um tipo de acesso diferente daquele que tínhamos no passado, mas um tipo muito mais generalizado de acesso. Mais de três quartos da população mundial tem acesso a um telefone celular.[51] A telefonia móvel é muito diferente dos computadores em nossas mesas ou até mesmo dos nossos laptops. Eles funcionam como telefone, enviam mensagens de texto e ainda possuem câmeras fotográficas, filmadoras, computadores, portais *web*, plataformas de jogos, e ainda assim são suficientemente pequenos para caber no bolso de uma camisa. Podemos levá-los para onde quisermos para ter acesso de via dupla, sempre ligados, e sempre conectados ao mundo digital. A mobilidade está mudando a forma como dados e serviços são acessados, assim como a *web* mudou a forma como eles são fornecidos e a computação em nuvem está mudando a forma como são processados e gerenciados. Por exemplo, um novo aplicativo móvel chamado "Agentto", desenvolvido no Brasil, ajuda a tornar as comunidades mais seguras, fornecendo aos indivíduos um canal baseado em localização em tempo real para notificar família, amigos e autoridades em meio a situações críticas, como acidentes, problemas de saúde, violência doméstica, sequestros e catástrofes.[52]

49. Mark Lyndersay, *Microsoft Evangelises the Cloud*, TRINIDAD & TOBAGO GUARDIAN (25 de outubro de 2012), http://www.guardian.co.tt/business-guardian/2012-10-24/ microsoft-evangelises-cloud.

50. VMware, *Business Agility and the True Economics of Cloud Computing*, *disponível em* https://www.vmware.com/files/pdf/accelerate/VMware_Business_Agility_ and_the_True_Economics_of_Cloud_Computing_White_Paper.pdf.

51. *Mobile Phone Access Reaches Three Quarters of Planet's Population*, WORLD BANK (17 de julho de 2012), http://www.worldbank.org/en/news/press-release/2012/07/17/ mobile-phone-access-reaches-three-quarters-planets-population.

52. AGENTTO, https://agentto.com/About.aspx (último acesso em 28 de setembro de 2013).

5. Segurança

É de se compreender que muitas organizações e indivíduos estão preocupados com a questão da segurança da nuvem. Na verdade, não há nenhuma razão técnica que impeça a nuvem de ser tão ou mais segura do que a computação tradicional. Em um estudo de 2012 feito com 70.000 quebras de segurança em 1.600 empresas, a AlertLogic concluiu que sistemas de computação nas instalações da organização eram mais vulneráveis a ataques do que aplicativos hospedados na nuvem.[53] Quarenta e seis por cento dos servidores corporativos foram afetados por ataques de "força bruta", em comparação com 39 por cento dos sistemas de nuvem.[54]

Como a Agência Europeia para a Segurança das Redes e da Informação (ENISA) reconheceu, "a computação em nuvem tem forte potencial para melhorar a segurança e a resiliência."[55] Apesar de regras robustas de privacidade de dados serem essenciais para que os usuários tenham confiança de que seus dados estarão seguros na nuvem, as tecnologias de nuvem podem, por si só, melhorar a segurança e a privacidade dos dados – especialmente para pequenas e médias empresas, que dispõem de conhecimentos e recursos limitados de segurança da informação. Muitas empresas de pequeno porte não têm os recursos necessários para implantar controles robustos de segurança física e técnica de forma sistemática, aplicar e testar *patches* de segurança, implementar soluções abrangentes de criptografia ou obter certificações de segurança e privacidade de informações. A computação em nuvem permite que essas organizações tenham as mesmas salvaguardas disponíveis para organizações de grande porte com orçamentos consideráveis para tecnologia de informação, equipe qualificada e instalações.[56]

Tendo em conta todos estes benefícios, deixa de ser surpreendente que os usuários estejam entusiasmados com a nuvem. A KPMG, por exemplo, concluiu que impressionantes 59 por cento dos holandeses responsáveis pelas tomadas de decisões e líderes de empresas concordam que "a computação em nuvem é o modelo de TI do futuro."[57] A maioria dos consumidores e empresários acreditam que essas tecnologias podem ajudar o governo a operar de forma mais eficiente e também produtiva.

---

53. Joe McKendrick, Cloud Apps Somewhat More Secure Than On-Premises Apps: Survey, FORBES, 19 de setembro de 2012, http://www.forbes.com/sites/joemckendrick/2012/09/ 19/cloud-apps-somewhat-more-secure-than--on-premises-apps-survey/

54. *Id.*

55. *Perguntas frequentes sobre o relatório "Cloud Computing: Benefits, risks and recommendations for information security,"* EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA) (último acesso em 19 de setembro de 2013), http://www.enisa.europa.eu/media/faq-on-enisa/ FAQ%20Cloud%20Computing.pdf.

56. *Ver* Tom Kelly, *SMEs must embrace the cloud to achieve global growth*, THE GUARDIAN (26 de abril de 2013), http://www.theguardian.com/media-network/media-net work-blog/2013/apr/26/clou-d-services-sme-businesses-growth?guni=Article:in%20 body%20link.

57. KPMG, FROM HYPE TO FUTURE: PESQUISA DA KPMG SOBRE COMPUTAÇÃO EM NUVEM (2010), *disponível em* http://www.kpmg.com/ES/es/ActualidadyNovedades/ArticulosyPublicacio nes/Documents/2010-Cloud-Computing--Survey.pdf.

O desafio para a indústria de TI é saber como aproveitar esse entusiasmo e garantir a empresas e indivíduos que seus dados estão seguros na nuvem.

B. Um Papel Importante para a Regulamentação Equilibrada

Os reguladores podem ajudar a estender os benefícios da computação em nuvem para mais empresas e indivíduos, estabelecendo confiança nessa tecnologia, garantindo a privacidade e segurança de dados e esclarecendo incertezas jurídicas e de políticas públicas. Esta seção descreve os elementos gerais de uma política regulatória de privacidade e proteção de dados que promova a competitividade nacional na computação em nuvem.

1. Garantindo a Proteção da Privacidade

A nuvem não alcançará todo o seu potencial se os usuários não confiarem na tecnologia. Inúmeras pesquisas mostram que empresas e indivíduos continuam bastante preocupados com relação à privacidade e à segurança na nuvem. Por exemplo, uma pesquisa de 2010 feita pelo Fórum Econômico Mundial constatou que 90 por cento dos entrevistados na Europa consideram a privacidade como uma limitação "muito séria" à adoção da computação em nuvem.[58] Como pessoas e organizações em todo o mundo transferem informações de *desktops* para seus dispositivos móveis e para a nuvem, elas querem saber se seus dados permanecerão seguros e protegidos.

As agências reguladoras podem estabelecer políticas regulatórias claras e justas para ajudar a garantir que usuários, empresas e indivíduos não percam suas proteções de privacidade ao mover dados para a nuvem. Como o Conselheiro Geral da Microsoft, Brad Smith, declarou na 34º Conferência Anual de Proteção de Dados e Reguladoras de Privacidade, realizada no Uruguai em outubro de 2012, "Precisamos de clareza para que todos saibam o que precisam fazer, e que as empresas que agem com responsabilidade não sejam prejudicadas por aquelas que não agem de forma responsável. A regulamentação cria a base propícia para que haja igualdade de condições."[59] As políticas regulatórias devem se concentrar nos objetivos principais, que consistem em garantir a segurança de dados, proteger a privacidade do consumidor e promover a confiança na nuvem.

58. Joanna Gordon et al., *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation*, World Economic Forum (2010), *disponível em* http://www3.weforum.org/docs/WEF_ITTC_FutureCloudComputing_Report_2010.pdf.

59. Brad Smith, Conselheiro Geral e Vice-Presidente Executivo, Microsoft Corporation, Palestra de Abertura da 34ª Conferência Internacional de Responsáveis pela Proteção de Dados e Privacidade: *Putting People First: Moving Technology and Privacy Forward* (23 de outubro de 2012), *disponível em* http://www.microsoft.com/en-us/news/download/legal/10-23puttingpeoplefirst.pdf.

Mas as regras dos legisladores não bastam. A autorregulação da indústria e a inovação baseada no mercado também são fundamentais para garantir a proteção da privacidade. A autorregulação, na forma de padrões da indústria, ajuda a tecnologia a avançar mais rápida e globalmente do que o regulamento faria por si só. Por exemplo, as partes interessadas desenvolveram um projeto de padrões internacionais, o ISO/IEC 27018, pelo qual um provedor de nuvem pode demonstrar aos clientes e reguladores que manipula dados pessoais corretamente e que garante a confidencialidade, integridade e disponibilidade desses dados.[60]

O mesmo ocorre com a inovação no mercado, onde há uma oportunidade para as empresas experimentarem coisas novas para saber o que os consumidores querem e se os consumidores realmente quiserem aquilo que elas estão oferecendo, haverá uma oportunidade de crescimento para essas empresas.

2. Encorajando Maior Transparência

Da mesma forma, uma política regulatória pode fornecer aos *clientes* as informações que eles tanto necessitam e buscam sobre a nuvem. Não basta que os provedores de serviços na nuvem afirmem que seus serviços são privados e seguros. Os clientes devem ser detalhadamente informados sobre isso. Regulamentações de privacidade e segurança de dados podem exigir que prestadores de serviços na nuvem mantenham por escrito informações abrangentes sobre seus programas de segurança e salvaguardas, forneçam resumos desses programas para os clientes e divulguem suas práticas de privacidade a qualquer cliente cujas informações pessoais sejam coletadas.

Transparência é especialmente importante, dada a proliferação de serviços de nuvem "gratuitos", nos quais o provedor lucra com a extração de dados que lhe foram confiados pelos usuários e com a venda desses dados a anunciantes ou a outros terceiros. Apesar de não haver nada intrinsecamente errado com esses modelos de negócios baseados em publicidade, os usuários precisam entender a natureza dos dados que estão sendo coletados e como eles são usados para que os usuários possam tomar decisões bem informadas antes de aceitar uma barganha. Em alguns casos, consumidores e pequenas e médias empresas podem decidir não fornecer dados a um serviço gratuito, se a natureza dos dados coletados e a forma

60. *Ver* Information technology — Security Techniques — Code of practice for PII protection in public cloud acting as PII processors, ISO/IEC DIS 27018 (Int'l Org. for Standardization 2013), *disponível em* http://www.iso.org/iso/catalogue _detail.htm?csnumber=61498.

como são divulgados a terceiros colocar em risco sua reputação, sua privacidade pessoal ou seus interesses econômicos. Com efeito, os consumidores estão cada vez mais atentos ao fato de que as informações fornecidas a um serviço de nuvem podem ter consequências em outros contextos; por exemplo, preocupações sobre o uso, pelo empregador, de contas de mídia social de candidatos a uma vaga de emprego levaram políticos nos Estados Unidos a estudar uma legislação que limitasse esse tipo de uso.[61] Em uma era em que os usuários devem considerar as consequências de seus "rastros" digitais, a divulgação honesta de práticas de uso de dados e privacidade pelos provedores de nuvem é absolutamente essencial.

3. Possibilitando e Protegendo Fluxos de Dados Entre Fronteiras

Conseguir migrar dados entre várias áreas geográficas permite que provedores reúnam seus recursos de TI em grupos, reduzam suas despesas administrativas e aumentem seu poder de compra. Essa medida também resulta em benefícios de custo e eficiência para os consumidores, assim como para o meio-ambiente, uma vez que o número de *data centers* usados também diminui.[62] Especialmente importante é a escala necessária para disponibilizar um serviço de nuvem viável no ponto de preço mais acessível. Apesar de cada novo servidor usado no serviço de nuvem pública gerar considerável redução de custos, há uma redução ainda maior, uma vez que pelo menos 10.000 servidores são empregados em uma nuvem pública.[63] Do ponto de vista operacional, provedores de computação de nuvem transferem dados entre *data centers* a fim de oferecer serviços essenciais aos clientes, incluindo suporte técnico e desenvolvimento de produtos 24 horas por dia. Do mesmo modo, a transferência de dados é essencial para *backup* de dados e resiliência. Como observado em um relatório recente do mercado de seguros Lloyd's, "o mundo digital ainda é suscetível a desastres físicos, tais como inundações, terremotos e furacões", e, portanto, a "concentração geográfica" de dados pode aumentar o risco de perda.[64]

---

61. *Ver, por exemplo*, *Employer Access to Social Media Usernames and Passwords 2013*, Nat'l Conference of State Legislatures, http://www.ncsl.org/issues-research/ telecom/employer-access-to-social-media-passwords-2013.aspx (último acesso em 23 de setembro de 2013).

62. *Ver* Niels Soelberg, *The Economics of Cloud Computing for the EU Public Sector*, http://www.microsoft.com/eu/transforming-business/article/the-economics-of-cloud-computing-for-the-eu-public-sector.aspx (último acesso em 23 de setembro de 2013).

63. Federico Etro, The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe An application of the Endogenous Market Structures Approach to a GPT innovation (Fevereiro de 2009).

64. Lloyd's, Digital Risks - Views of a changing risk landscape, Lloyd's Emerging Risks Team Report (Outubro de 2009), *disponível em* http://www.lloyds.com/~/media/lloyds/reports/emerging%20risk%20reports/digital-risksreport_october2009v2.pdf.

A nuvem é um veículo perfeito para assegurar que essas informações críticas não desapareçam para sempre em consequência de catástrofes naturais ou provocadas pelo homem, uma vez que o serviço de nuvem, por sua natureza, não concentra o *backup* de dados no mesmo lugar; em vez disso, ele distribui os *backups* em diferentes partes do mundo para maximizar a eficiência e continuidade do serviço e reduzir os custos para o consumidor.

Regras restringindo a transferência de dados e informações através das fronteiras, no entanto, não acompanham a realidade atual da computação baseada em banda larga. Apesar de não ser esta a intenção, essas regras limitam a inovação e o desenvolvimento econômico, que normalmente seria viabilizado pela nuvem, e muitas vezes não produzem qualquer benefício correspondente à privacidade do consumidor. Como a Comissão Europeia reconheceu: "há uma necessidade geral de melhorar os mecanismos atuais para as transferências internacionais de dados", tendo em vista o vertiginoso aumento nos serviços prestados através da Internet desde que a Diretiva de Proteção de Dados foi adotada há 15 anos.[65] Da forma como está, a Diretiva restringe consideravelmente a transferência de dados pessoais da Europa para qualquer país cujas leis domésticas não forneçam um nível de proteção que a UE considere "adequado". Na prática, apenas aqueles países que fornecem os mesmos métodos precisos de proteção que a UE, como a Argentina e Uruguai, têm sido considerados adequados.[66] No total, somente sete países são considerados adequados, juntamente com cinco microestados ou territórios dependentes, tais como a Ilha de Man.[67] Assim, na prática, o regime de adequação comunitário tem limitado a circulação de dados entre fronteiras, mesmo quando isso compromete os benefícios alcançados pela computação em nuvem.

A exceção "*Safe Harbor*" (porto seguro) adotado pela UE para os Estados Unidos, no entanto, reconhece que apesar de os Estados Unidos não empregarem os mesmos métodos precisos de proteção de privacidade que a UE, não é necessário negar a um país o status "adequado" e recusar os benefícios da infraestrutura em nuvem dos principais mercados, tais como os Estados Unidos.[68]

65. *Ver A comprehensive approach to personal data protection in the European Union*, COM (2010) 609 final (11 de abril de 2010), *disponível em* http://ec.europa.eu/justice/ news/consulting_public/0006/com_2010_609_en.pdf.

66. *Decisões da Comissão sobre a adequação da proteção de dados pessoais em outros países*, EUROPEAN COMMISSION JUSTICE, http://ec.europa.eu/justice/data-pro tection/document/international-transfers/adequacy/index_en.htm (última atualização em 16 de julho de 2013).

67. *Id.*

68. Visão Geral do *Safe Harbor* EUA – UE, EXPORT.GOV, http://export.gov/safeharbor/ eu/eg_main_018476.asp (última atualização em 1 de julho de 2013).

Em vez disso, outros mecanismos podem ser desenvolvidos para permitir o fluxo livre, porém seguro, de dados entre fronteiras. Sob o status de *Safe Harbor*, empresas dos Estados Unidos atestam que importarão dados da UE somente em condições que estejam em conformidade com as leis de privacidade da UE.[69] Nem todos os países que limitam a transferência de dados para países "adequados", no entanto, adotaram mecanismos alternativos de conformidade, como a política de *Safe Harbor* adotada pela UE. Estabelecer esse tipo de mecanismo nos diversos países latino-americanos que adotaram as restrições para transferência de dados segundo o modelo da UE pode ser a chave para o desenvolvimento de serviços robustos de computação em nuvem na América Latina.[70]

Independentemente da natureza de uma restrição excessivamente rigorosa para dados internacionais – se é o resultado de uma proibição expressa na exportação de dados, uma limitação baseada em uma exigência de "adequação" ou de leis inconsistentes entre jurisdições, a consequência involuntária de colocar uma cerca nacional em torno da nuvem de um país é diminuir o investimento, reduzir o comércio e privar consumidores e empresas dos benefícios da computação em nuvem e de outras inovações.

Alternativamente, forçar um provedor a armazenar dados localmente, numa jurisdição que impõe restrições ao fluxo livre de dados, impede que esse provedor proporcione aos clientes os benefícios de custo e serviço resultantes da capacidade de migrar os dados para o local de armazenamento mais eficiente. Também deixarão de existir os potenciais benefícios ambientais e de eficiência energética decorrentes da consolidação de recursos em um número menor de *data centers*.[71] Em poucas palavras, o desejo de estabelecer *data centers* entra em conflito com os benefícios almejados, porém associados à economia de escala da computação em nuvem. Na medida em que não há qualquer ganho a curto prazo em forçar provedores de nuvem a construir *data centers* locais como uma condição para se

69. Visão Geral do *Safe Harbor* EUA – UE, EXPORT.GOV, http://export.gov/safeharbor/ eu/eg_main_018476.asp (última atualização em 1 de julho de 2013).

70. A Comissão Europeia (CE) publicou recentemente uma série de recomendações destinadas a melhorar o funcionamento do mecanismo de *Safe Harbor*. Embora as partes interessadas tenham diferentes pontos de vista quanto a essas recomendações, a CE reconheceu que o *Safe Harbor* é um componente importante da relação comercial UE-EUA, da qual dependem empresas de ambos os lados do Atlântico." Ao fazer suas recomendações, a CE reconheceu ainda que qualquer revogação do *Safe Harbor* seria imprudente, observando que isso "afetaria negativamente os interesses das empresas associadas presentes na UE e nos EUA", e concluindo que "o *Safe Harbor* deveria, ao contrário, ser reforçado. " *Ver* EUROPEAN COMMISSION JUSTICE, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: REBUILDING TRUST IN EU-US DATA FLOWS 6 (27 de novembro de 2013), *disponível em* http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

71. *Ver*Soelberg, *supra* nota 62.

fazer negócios, a longo prazo tais ganhos serão mínimos frente às oportunidades perdidas, uma vez que muitos provedores de nuvem simplesmente optaram por não disponibilizar serviços em nuvem no país. Além disso, os mandatos para instalar *data centers* locais produzem pouco benefício econômico dentro do país, já que essa exigência baseia-se na falsa premissa de que *data centers* físicos – ao contrário dos serviços que eles possibilitam – promovem o crescimento no número de empregos no setor.[72]

4. Harmonização de Regras de Proteção de Dados e Interoperabilidade

A principal característica da nuvem é sua falta de limites físicos. Isso permite que usuários em qualquer país criem, acessem e compartilhem dados com pessoas do mundo inteiro. Essa falta de limites físicos infelizmente significa que um provedor de nuvem está potencialmente sujeito às leis de centenas de nações e milhares de jurisdições.[73] As leis de privacidade e segurança de dados variam muito.[74] Alguns países impõem algumas exigências rigorosas, como avisos e consentimento, enquanto outros não impõem nenhuma.[75] Alguns países limitam a transferência de dados para determinados países, enquanto outros não têm qualquer restrição quanto ao fluxo de dados.[76] Alguns países exigem que as empresas guardem cuidadosamente as informações pessoais, enquanto outros dispensam tais garantias.[77]

Os regulamentos e as leis de privacidade têm variado ao longo de décadas. Mas a ascensão da computação em nuvem ampliou os problemas causados por essas inconsistências. Um provedor de nuvem verdadeiramente global deve assegurar-se de que está atendendo as exigências de todas as leis de privacidade e segurança de dados, mesmo que essas leis sejam conflitantes entre si. Precisamos de regras que possam ser aplicadas de forma cada vez mais consistente nos países e continentes. Seria irrealista esperar que todos os países adotem regras idênticas de proteção de dados e privacidade. Mas se eles fizerem um esforço para harmonizar determinados requisitos, reduziriam a incerteza para provedores de serviços em nuvem.

72. *Ver* James Heaney, *Yahoo Aims to Expand Data Center in Lockport*, BUFFALO NEWS (4 de abril de 2011, 12:01 AM), http://www.buffalonews.com/article/20110404/CITY ANDREGION/304049993 ("*Data centers*, entretanto, não são considerados mecanismos econômicos significativos.").

73. *Ver* Juliette Garside, *How global laws protect your data*, THE GUARDIAN (16 de outubro de 2011, 7:01 PM), http://www.theguardian.com/cloud-technology/global-laws-pro tect-your-data.

74. *Ver* Constance Gustke, *Which countries are better at protecting privacy*, BBC (26 de junho de 2013), http://www.bbc.com/capital/story/20130625-your-private-data-is-showing.

75. *Id.*

76. *Id.*

77. *Id.*

Só através da colaboração entre governos é possível criar consistência entre as políticas regulatórias que são indispensáveis para que a nuvem funcione. Governos poderiam começar trabalhando para desenvolver regras que facilitarão os fluxos de dados através das fronteiras nacionais e regionais. Alternativamente, os governos poderiam trabalhar juntos para desenvolver princípios comuns para determinar quando um país tem jurisdição sobre os dados armazenados na nuvem.

Pode ser mais eficaz para os governos ao longo do tempo, buscar políticas multilaterais sobre estas questões na forma de tratados ou instrumentos internacionais similares. Apesar de esta opção exigir, sem dúvida, recursos e mediação diplomática, ela talvez ofereça a melhor chance de lidar com as necessidades legítimas do governo de maneira coerente, assegurando que os interesses de empresas e consumidores em privacidade sejam atendidos em uma escala global.

Uma opção menos formal seria envolver os países bilateralmente ou regionalmente em consultas e construção de consensos para melhor harmonizar seus respectivos sistemas de proteção de dados e solucionar problemas de acesso de dados. Esse tipo de envolvimento pode aumentar a visibilidade desses problemas e preparar o caminho para um solução mais formal e de longo prazo. Na Ásia, por exemplo, o progresso alcançado pelo Programa de Cooperação de Desenvolvimento ASEAN-Austrália, para conciliar os sistemas legais e de *e-commerce* com os Projetos Pathfinder e o *APEC Privacy Framework,* criou uma plataforma sólida para desenvolver soluções para abordagens jurisdicionais divergentes relacionadas às políticas de tecnologia. Além disso, os padrões voluntários ISO 27001/27002 garantem a segurança da informação em empresas do mundo inteiro. Tais discussões regionais multipartidárias apresentam uma oportunidade de crescimento da computação em nuvem e de ampliação de seus benefícios em diversos níveis, por toda uma região.

À medida que as nações latino-americanas adotam novas leis e regulamentos de proteção de dados, elas também deveriam considerar a interoperabilidade uma prioridade. Como ponto de partida, os países devem assegurar que haja um sistema interoperável na região. Por exemplo, em geral, empresas de computação em nuvem deveriam ser capazes de esperar que se elas cumprirem com as regras e regulamentos mexicanos sobre privacidade de dados, não precisarão fazer mudanças significativas em suas práticas para que possam cumprir também com as regras e regulamentos do Chile, ou vice-versa. Um sistema harmonizado e interoperável também daria à região uma voz clara e de maior peso no diálogo global sobre regulamentos de proteção de dados e nuvem.

O objetivo final deve ser garantir que as regras de proteção de dados nos países latino-americanos sejam interoperáveis com as de outras regiões, incluindo os EUA, a UE e Ásia. Como temos observado, determinações rígidas de "adequação" criam complicações desnecessárias para os fluxos de dados que tornam a nuvem uma realidade.

5. Fortalecimento das Leis Contra Delitos Cibernéticos

Ao combater e prevenir delitos cibernéticos, os governos podem ajudar a construir a confiança do consumidor na nuvem. Por "delitos cibernéticos", estamos nos referindo a uma variedade de atividades criminosas online. Os três tipos de delitos cibernéticos que representam a maior ameaça para a nuvem são: 1) crimes contra indivíduos, como ataques a crianças, 2) crimes contra nações, como o terrorismo, e 3) crimes econômicos, como fraudes de cartão de crédito.[78]

Combater o delito cibernético sempre foi um problema global, mas a computação em nuvem reforça essa concepção. Como a vítima muitas vezes está em uma jurisdição, o *data center* localiza-se em outra e o infrator age em uma terceira, deveria haver um mecanismo eficaz de cooperação entre as agências policiais da América Latina, da UE, dos EUA e de outras regiões. Há uma necessidade de normas claras e consistentes para assegurar a produção, conservação e preservação de dados em investigações que envolvem múltiplas jurisdições; o investimento em *know-how* tecnológico para a aplicação da lei local; e a cooperação na criação de agências internacionais, por meio das quais os dados sobre crimes cibernéticos seriam compartilhados, havendo um ponto central de contato global para avaliar tendências e fazer conexões que ajudariam a identificar os infratores.

Em suma, através de um sistema coerente de políticas regulatórias que protejam a privacidade e instalem a confiança do consumidor, os governos podem ajudar a promover a competitividade nacional por meio da computação em nuvem.

III. DESAFIOS, TENDÊNCIAS E A EXPERIÊNCIA INICIAL DA REGULAMENTAÇÃO DA NUVEM

A nuvem não só apresenta oportunidades sem precedentes, como também novas perguntas de segurança e privacidade para a indústria, os legisladores e consumidores. Todas as partes interessadas devem identificar esses desafios e

78. *Ver, por exemplo*, Elinor Mills, *Cybercrime moves to the cloud*, CNET (30 de junho de 2012, 6:00 AM), http://news.cnet.com/8301-1009_3-57464177-83/cybercrime-moves-to-the-cloud/ (discute como a nuvem poderia ser alvo de criminosos cibernéticos); *ver também Top Threats to Cloud Computing V1.0*, Cloud Security Alliance (Março de 2010), *disponível em* https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

determinar qual é a maneira mais eficaz de abordá-los, sem deixar de aproveitar todo o potencial da nuvem para promover inovação local e prosperidade econômica local.

A. A Computação em Nuvem Apresenta Importantes Questões Relacionadas à Privacidade e Segurança de Dados

A necessidade de tomar decisões ponderadas é especialmente verdadeira nesta era de "big data", que envolve a coleta, o gerenciamento e uso de dados em grande escala. Mesmo quando há informações isoladas, que por si só são relativamente inócuas, esses milhares de *bits* de dados podem "começar a pintar um quadro da vida de uma pessoa" quando agregados.[79] Em um exemplo particularmente vívido, o *New York Times* explicou como uma grande rede varejista foi capaz de prever que uma adolescente estava grávida – e enviar a ela cupons de desconto de produtos relacionados – antes mesmo que seu pai soubesse, somente com base no seu histórico de compras.[80] Redes de publicidade online têm acesso a um conjunto muito mais amplo de informações. Pesquisadores na Universidade de Stanford, por exemplo, descobriram uma empresa de publicidade que usou um script para determinar o histórico de navegação dos usuários e combinar as páginas visitadas com uma grande variedade de segmentos de interesse, incluindo temas delicados como negociação de dívidas.[81]

As organizações que estão migrando para a nuvem – sejam elas agências governamentais, empresas, escolas ou outras instituições – estão preocupadas com a privacidade e a segurança de seus dados, a conformidade regulatória e políticas de uso de dados de provedores de serviços em nuvem. Uma pesquisa recente realizada pela Cloud Security Alliance descobriu que usuários de organizações consideram a segurança das informações a principal limitação à adoção da nuvem.[82]

Usuários individuais têm preocupações semelhantes. Eles querem ter uma garantia de que seus dados estarão seguros e protegidos contra hackers, e que poderão controlar quem tem acesso às suas informações pessoais. Estabelecer a confiança é fundamental para promover o acesso e incentivar o investimento.

---

79. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 Minn. L. Rev. 1137, 1141 (2002).

80. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times (16 de fevereiro de 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

81. Jonathan R. Mayer & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology* (2012), *disponível em* https://cyberlaw.stanford.edu/files/publication/files/ trackingsurvey12.pdf; Jonathan Mayer, *Tracking the Trackers: To Catch a History Thief*, Cis (19 de julho de 2011, 4:20 AM), http://cyberlaw.stanford.edu/node/6695.

82. Joe McKendrick, *Cloud's Full Impact is Still About Three Years Away, Survey Predicts*, Forbes (12 de outubro de 2012), http://www.forbes.com/sites/joemckendrick/2012/10/ 03/clouds-full-impact-is-still-about-three-years-away--survey-predicts/.

Para que a nuvem realmente tenha sucesso, os consumidores devem se sentir tão confortáveis armazenando suas informações lá quanto estariam se estivessem usando suas unidades pessoais de disco rígido.

B. Tendências Regulatórias

A Argentina foi pioneira em 2000, quando promulgou as primeiras normas abrangentes de proteção e privacidade da América Latina.[83] Essas regulamentações desenvolveram a confiança do consumidor na Internet e ajudou o setor de tecnologia de informação do país a prosperar. Mas muitos desses regulamentos não se aplicam à nuvem hoje. Infelizmente, alguns países da região continuam adotando leis que limitam os benefícios da nuvem. Nações com leis baseadas em modelos desenvolvidos na década de 1990 devem modernizar suas regras de proteção de dados e privacidade para desenvolver a confiança na nuvem e manter a competitividade nacional. Vivemos em um mundo digital que mudou radicalmente na última década. As leis da era "pré-nuvem" não lidam adequadamente com os requisitos de privacidade e segurança que hoje fazem parte da nossa realidade.

Regulamentos consistentes de proteção de dados e privacidade podem estabelecer uma linha de base útil para todos os provedores de serviços em nuvem. Regulamentações equilibradas poderiam estabelecer a confiança do consumidor na nuvem e ajudar a promover o crescimento desta tecnologia notável. Em vez de articular requisitos regulatórios específicos, acreditamos que seria mais útil discutir duas características gerais para uma regulamentação efetiva para nuvem.

Em primeiro lugar, a regulamentação deve permitir que os dados fluam livremente entre as fronteiras, em circunstâncias que garantam que aquele que está importando os dados tomará medidas para proteger e dar segurança aos dados pessoais. Assim como a Internet sobre a qual está baseada, a nuvem é mundial. Serviços em nuvem podem cruzar dezenas ou centenas das fronteiras nacionais e, no caminho, dezenas ou centenas de políticas regulatórias. Esta colcha de retalhos de regulamentações requer uma atualização substancial.

Em segundo lugar, a regulamentação deve proteger a privacidade e assegurar que a nuvem tenha proteção contra acesso não autorizado. Como demonstrado acima, confiança é essencial para o sucesso da nuvem. Privacidade e segurança são citados como os dois principais obstáculos à adoção da nuvem de forma mais ampla.[84]

---

83. *Ver* Maxim Gakh, *Argentina's Protection of Personal Data: Initiation and Response*, 2 I/S: J. L. & Pol'y for Info. Soc'y 781 (2006) (discute a Lei de Proteção de Dados da Argentina e o efeito de sua promulgação em outros países).

84. World Economic Forum, Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-Driven Transformation (2010), *disponível em* http://www.weforum.org/pdf/ip/ittc/Exploring-the-future-of-cloud-computing.pdf.

Uma nuvem segura e aberta é uma nuvem protegida contra hackers e ladrões, mas que também serve como um reservatório de informações que atende todas as pessoas por meio de serviços contínuos, de baixo custo e acessíveis a partir de dispositivos sempre conectados.

Os governos sabiamente começaram a analisar propostas que protegem a privacidade dos consumidores na nuvem através de um mecanismo orientado a resultados. A Comissão Europeia, por exemplo, sugeriu que um princípio de "responsabilidade" constasse expressamente no sistema de proteção de dados da UE.[85] Sob um regime baseado na responsabilidade, requisitos e padrões de proteção de dados são previstos em lei, mas recai sobre as organizações grande parte da responsabilidade de determinar a melhor maneira de cumprir essas normas na prática. É importante, contudo, que o benefício de uma abordagem de responsabilidade não seja desperdiçado pela simples imposição de uma exigência determinando que organizações sejam responsabilizadas, além de obedecerem todas as regras prescritivas da UE já existentes. Em vez disso, a responsabilidade deve ser usada no lugar de regras prescritivas, uma questão que o *Information Commissioner* (Diretor de Informações) do Reino Unido levantou no início deste ano, quando se opôs a aspectos das regras de proteção de dados propostas pela UE.[86]

Nesse mesmo sentido, a legislação recomendada pelo Departamento de Comércio dos EUA criaria uma exceção *safe harbor* de ações de execução governamental pelas empresas que aderissem de forma voluntária a códigos de conduta com força legal, elaborados por meio de processos envolvendo diversas partes interessadas. O Departamento de Comércio enfatizou com propriedade que essa abordagem flexível do *Safe Harbor* não diminuiria as proteções para o consumidor, observando que "[d]eixar de obedecer as provisões do código voluntário, porém com força legal, poderia levar a uma ação de execução pela FTC ou por um procurador geral do Estado."

C. A Abordagem da Microsoft

Regulamentações, por si só, não vão desenvolver o nível necessário de confiança do consumidor na nuvem. A indústria deve ter um diálogo permanente com o consumidor sobre privacidade na nuvem. A Microsoft está comprometida

85. *Data Protection Accountability: The Essential Elements*, The Centre For Information Policy Leadership (Outubro de 2009), *disponível em* http://www.huntonfiles .com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

86. Liat Clark, *ICO Commissioner Slams EU Data Protection Directive*, Wired UK (7 de fevereiro de 2013), http://www.wired.co.uk/news/archive/2013-02/07/ico-against-eu-data-protection ("Queremos que isso seja definido em termos de resultados, e não de processos regulatórios.").

em assumir um papel proativo e responsável nesta área. Acreditamos firmemente que práticas de privacidade na nuvem seriam beneficiadas pelos serviços que informam os consumidores e comparam ofertas. A título de analogia, no setor automotivo esse tipo de diálogo tem sido bem-sucedido para estimular a indústria a inovar na área de segurança através de iniciativas governamentais para informar o público, bem como revistas e sites que classificam os carros com base em padrões de segurança e opiniões do consumidor. Um diálogo similar no contexto da computação em nuvem poderia aumentar a capacidade de reação da indústria frente às necessidades de privacidade.

A Microsoft, por exemplo, obtém *feedback* dos clientes através de diversos meios, incluindo testes de usabilidade, pesquisas, grupos de discussão e outros tipos de pesquisa de campo. A empresa também criou um programa chamado *Customer Experience Improvement Program* (CEIP), através do qual clientes podem voluntariamente compartilhar informações online sobre programas da Microsoft e relatar qualquer problema que venham a encontrar. Essas informações ajudam a Microsoft a inovar e melhorar a experiência do usuário de forma geral, incluindo sua privacidade e segurança, cuja proteção a Microsoft está comprometida em garantir.

Entre outras coisas, a Microsoft aprendeu com esse *feedback,* que os clientes querem entender melhor quais dados estão sendo coletados e como estão sendo usados. Em resposta, estamos trabalhado com afinco para fornecer informações, de forma clara e fácil de entender, acerca de nossas práticas de privacidade e segurança. Por exemplo, a Microsoft criou a Central de Confiabilidade do Office 365 para fornecer um nível de transparência sobre práticas de segurança e privacidade de dados líder na indústria. A Central de Confiabilidade fornece a clientes e outras partes interessadas explicações claras e fáceis de entender sobre o que a Microsoft faz com dados armazenados na nuvem — incluindo a forma como são coletados, em quais circunstâncias eles podem ser acessados, para onde os dados fluem e como o cliente pode receber informações adicionais de segurança, privacidade e auditoria.[87] A Central de Confiabilidade é uma inciativa única na indústria e fez da Microsoft a líder em transparência na nuvem. Em contraste com alguns provedores de serviços em nuvem que não são totalmente transparentes sobre suas práticas de uso de dados, a Microsoft declara de forma clara que utilizará os dados de uma empresa cliente *somente* para fornecer os serviços solicitados pelo cliente, e não para se beneficiar comercialmente.

87. *Microsoft Office 365 Trust Center*, Microsoft Corp., http://office.microsoft .com/en-us/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx (último acesso em 24 de novembro de 2013).

Quando intimada ou legalmente obrigada por governos a fornecer informações de clientes, a posição da Microsoft é clara: a Microsoft acredita que os clientes devem controlar suas próprias informações, na medida do possível. Da mesma forma, se uma entidade governamental aborda a Microsoft diretamente para obter informações hospedadas em nome de clientes do Office 365, por exemplo, a Microsoft tentará, em uma primeira instância, redirecionar aquela entidade para entrar em contato com o próprio cliente e, assim, dar ao cliente a oportunidade de determinar como prefere responder. Se, no entanto, a Microsoft tiver que responder a essa demanda judicialmente, a Microsoft somente oferecerá as informações pertencentes ao clientes do Office 365 quando a Microsoft for legalmente obrigada a fazê-lo.

A Microsoft limita o fornecimento de informações que a Microsoft é obrigada a revelar, usando esforços razoáveis para notificar o cliente com antecedência sobre qualquer divulgação, a menos que a Microsoft esteja legalmente proibida de fazê-lo.[88]

Conforme declarou o Conselheiro Geral da Microsoft, Brad Smith, "sob nenhuma hipótese a Microsoft fornecerá a governos acesso direto ou irrestrito às chaves de criptografia ou aos dados do cliente. A Microsoft só extrai e fornece os dados especificamente exigidos por uma demanda judicial relevante."[89]

Além disso, à luz das recentes acusações relativas a vigilância dos dados de clientes por alguns governos, a Microsoft está tomando diversas medidas preventivas. Tais medidas incluem, por exemplo, fortalecer a criptografia em redes e serviços Microsoft (observando que dados do cliente no Office 365 e Outlook.com já contam com o benefício da criptografia quando viajam entre os clientes e a Microsoft) e melhorar a transparência do código de *software* da Microsoft (isto facilitará a garantia de que a engenharia de *software* da Microsoft não disponibiliza *back doors* nos produtos Microsoft, onde governos poderiam sorrateiramente explorar para acessar os dados privados dos clientes). Ao mesmo tempo, a Microsoft está se juntando a um grupo de empresas do setor, como a AOL, Apple, Facebook, Google, LinkedIn, Twitter e Yahoo para pedir reformas de vigilância governamental, que exigirão a adesão do governo a princípios específicos no que diz respeito a vigilância.[90]

Além da transparência, é evidente que os consumidores também querem

88. How We Use Your Data, *Microsoft Office 365 Trust Center*, Microsoft Corp., http://www.microsoft.com/online/legal/v2/?docid=23 (último acesso em 24 de novembro de 2013).

89. Brad Smith, *Responding to Government Legal Demands for Customer Data*, Microsoft on the Issues, (16 de julho de 2013), http://blogs.technet.com/b/microsoft_on_ the_issues/archive/2013/08/30/standing-together-for-greater--transparency.aspx.

90. Brad Smith, *Protecting Customer Data from Government Snooping*, The Official Microsoft Blog, (4 de dezembro de 2013), http://blogs.technet.com/b/microsoft_blog/ archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx.

escolher e controlar a forma como seus dados são usados — particularmente por empresas terceiras. Novamente, estamos trabalhando com afinco para responder.

O Internet Explorer fornece o recurso de *Tracking Protection* (Proteção Contra Rastreamento). Na Internet dos dias de hoje, os sites estão extraindo cada vez mais conteúdos, como imagens e texto, de sites de terceiros. Embora esta seja uma característica comum do design moderno da *web*, que permite que os provedores online melhorem seus sites e serviços, os usuários às vezes não estão cientes de que eles podem ser rastreados por terceiros através do conteúdo presente nas páginas da rede. Especificamente, os usuários poderão criar Listas de Proteção Contra Rastreamento, que permitem limitar o compartilhamento de seus dados a determinados sites ou categorias de sites. O usuário pode incluir qualquer site que desejar nessas listas e, no futuro, as pessoas provavelmente poderão escolher Listas de Proteção contra Rastreamento criadas por todos os tipos de empresas e organizações – de defensores de privacidade a empresas de segurança e grupos comerciais e publicitários. É importante lembrar que a Proteção Contra Rastreamento coloca os usuários no controle sem empregar mecanismos intrusivos que desvirtuam a experiência online, tais como interromper os usuários centenas de vezes ao dia para solicitar seu consentimento cada vez que um cookie é implantado.[91] A *European Privacy Association* (Associação Europeia de Privacidade) elogiou recentemente a proteção contra rastreamento pela contribuição para "a criação de um mercado online voltado para as necessidades dos consumidores e atenta às suas preocupações com a privacidade".[92]

A Microsoft oferece aos consumidores níveis semelhantes de escolha e controle através de nossos serviços e tecnologias. O Windows Phone 8, por exemplo, inclui um recurso de "localização geográfica" que permite ao consumidor tirar vantagem da crescente gama de serviços e aplicativos baseados em localização disponíveis no mercado. No entanto, nenhum aplicativo pode ter acesso às informações de localização a menos que o consumidor tenha consentido. Aplicativos que usam a localização do consumidor também são obrigados a permitir que o usuário desative esse acesso posteriormente – e os consumidores têm a opção de desligar o recurso de localização de todos os seus aplicativos.

A Microsoft também fornece aos clientes corporativos ferramentas de controle sofisticadas do uso de informações delicadas dentro de suas próprias organizações – por meio de inovações como o Windows 8 *BitLocker* e o *BitLocker To Go*, que criptografam dados em computadores e dispositivos USB portáteis e, assim,

91. Encontre mais informações sobre nosso recurso de proteção contra rastreamento em *IE9 and Privacy: Introducing Tracking Protection*, IEBLOG (7 de dezembro de 2010, 1:10 PM), http:// bit.ly/ietpl.

92. European Privacy Association, *Protection list: on the Right Track*, EPA NEWS (21 de janeiro de 2011), http://www.europeanprivacyassociation.eu/agenda_news.php?func tion=read&id=36.

impedem o acesso a dados delicados de uma organização se o dispositivo de um funcionário for perdido ou roubado.[93]

Em suma, a Microsoft está comprometida em manter a liderança no setor em relação à privacidade na nuvem. Por quê? Além das fortes convicções da empresa sobre privacidade e segurança, o modelo de negócios da Microsoft – baseado em receitas geradas com a venda de serviços e *software* inovadores – faz com que a empresa se esforce para proteger a privacidade dos seus usuários. Em contraste, alguns provedores de nuvem geram receitas quase que exclusivamente através da extração de dados de consumidores obtidos através de e-mails, pesquisas online, etc., para então servir os clientes publicitários de tais companhias (como diz o ditado: "se você tem um produto de graça, então *você* é o produto").[94] Isso leva a incentivos e abordagens muito diferentes em relação à privacidade. Por causa do modelo de negócios da Microsoft, a empresa acredita que a privacidade tem um grande valor comercial para os usuários e que devemos competir com outras empresas do setor para oferecer a melhor proteção disponível.

É claro que, apesar das ofertas dos concorrentes produzirem muitos benefícios em termos de privacidade, a colaboração e autorregulação do setor também são fatores críticos para promover a privacidade online – um ponto que a Comissão Europeia reconhece em sua Agenda Digital para a Europa.[95] É por isso que a Microsoft compartilha com parceiros e concorrentes as diretrizes de privacidade que adotamos quando desenvolvemos *softwares* e serviços online.[96]

Desde que a Microsoft disponibilizou essas diretrizes pela primeira vez em 2006, elas contribuíram significativamente para a principal certificação de privacidade profissional no setor de TI (*Certified Information Privacy Professional for IT,* ou *CIPP/ IT*) e ajudaram a moldar os padrões internacionais de privacidade. Vemos uma série de oportunidades para reforçar o diálogo com parceiros da indústria sobre autorregulação.

---

93. Para obter mais informações sobre ferramentas de segurança fornecidas no Windows 8, *ver* http://www.microsoft.com/security/pc-security/windows8.aspx. Além disso, a Microsoft certifica seus serviços online de acordo com os padrões de segurança ISO 27000 que, entre outras coisas, estabelecem diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação dentro de uma organização.

94. Bryan Cunningham, *Google's data mining raises questions of national security*, The Guardian (15 de outubro de 2012, 11:40 AM), http://www.theguardian.com/commentis free/2012/oct/15/google-data-mining-national-security ("A receita gerada pela combinação e monetização de tais dados – com a mineração de dados – explica como serviços em nuvem "gratuitos" conseguem ser gratuitos.").

95. *Ver* A Digital Agenda for Europe, Communication From the Commission to the European Parliament,the Council, The European Economic and Social Committee and the Committee of the Regions §2.3 (Trust and Security) (2010).

96. *Privacy Guidelines for Developing Software Products and Services Version 3.1*, Microsoft Corp. (2006) *disponível em* http://go.microsoft.com/?linkid=9746120.

Por exemplo, como dados de localização geográfica são cada vez mais coletados e usados para fornecer uma gama de serviços aos usuários, várias organizações estão trabalhando para criar códigos de conduta para ajudar a dissipar as preocupações dos legisladores em torno da coleta e do uso desses dados. A Microsoft continuará participando ativamente e apoiando esses esforços para a criação de práticas coerentes de proteção de privacidade na indústria.

IV. CONCLUSÃO

A computação em nuvem pode elevar as economias ao criar empregos e promover inovação, fomentar maior inclusão social e aumentar o padrão de vida da população, porque está disponível a um preço que, por si só, é muito inclusivo. Para viabilizar o crescimento econômico e os benefícios sociais que a computação em nuvem oferece, governos e indústria devem trabalhar juntos, tal como fizeram na promoção de eras de crescimento no passado que foram impulsionados pela inovação. A Microsoft está empenhada em fazer sua parte, tanto através de práticas de segurança e privacidade que lideram o mercado, quanto por meio do suporte a políticas regulatórias e de autorregulação do setor. Na América Latina, nos EUA, e em outras jurisdições, os governos já começaram a mapear as medidas necessárias, consultando uma ampla gama de grupos compostos por diversas partes interessadas. Encorajamos os governos a rever as políticas regulatórias, conforme for necessário, para melhorar o aproveitamento de suas plataformas de nuvem, de forma que os mais recentes recursos e serviços possam ser oferecidos aos seus cidadãos a um preço acessível, e que os inovadores locais possam compartilhar suas invenções com o mundo. No futuro, quando olharmos para trás, se dirá que essas políticas de proteção de dados que facilitaram a computação em nuvem foram responsáveis por servir às aspirações de um país por competitividade nacional.

* * *